NUREG/CR-2818
SAND82-7071
AN
Printed September 1982
CONTRACTOR REPORT

Protective Measures and Regulatory Strategies for Core Melt Accidents

International Energy Associates Limited
600 New Hampshire Ave., NW
Washington, DC 20037

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789

Prepared for
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

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-2818
SAND82-7071
AN
IEAL-194

Protective Measures and Regulatory Strategies for Core Melt Accidents

Prepared by
International Energy Associates Limited
600 New Hampshire Avenue, N.W.
Washington, D.C. 20037

Under Contract No. 62-7780

Prepared for
Sandia National Laboratories
Albuquerque, New Mexico 87185

Operated by
Sandia Corporation for the
U.S. Department of Energy

Printed September 1982

Funded by
Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Under Memorandum of Understanding, DOE 40-550-75
NRC FIN No. A1093

TABLE OF CONTENTS

PREFACE

The effort that is documented in this report was initiated in the summer of 1980, at a time when the Nuclear Regulatory Commission (NRC) was considering rulemaking that would likely require significant design modifications to nuclear power plants in order to deal with (i.e., prevent and/or mitigate) core-damage and core-melt accidents.

The original objective of this work was to determine the impact of such rulemaking on the structure and content of Title 10 of the Code of Federal Regulations and the associated NRC Division 1 Regulatory Guides. International Energy Associates Limited (IEAL) previously completed a similar task that considered only core-damage-accident rulemaking.

Early in our analysis, it became obvious that inclusion of core-melt accidents in the licensing process would change the same sections of the regulations and guides (although the detailed changes might be different) and possibly add new ones. But it also became apparent that the NRC appeared to be considering significant regulatory changes without a clear expression of why the changes were needed or what the NRC's strategy was regarding the overall level of safety of nuclear power plants.

As a result, the following report approaches the impact of core-melt rulemaking from the point-of-view that the NRC should first establish the need for core-melt rulemaking (e.g., based on risk) and, subsequently, a consistent strategy for implementing regulatory changes, if any.

The study proceeded at a relatively modest level of effort for close to a year, with NRC review of and comments on a draft report taking another eight months. During this period, the NRC began to focus on the concept of a safety goal for nuclear power plants using risk as the primary quantitative measure for such a goal. This development will allow, in our opinion, a more rational basis for evaluating the need for and extent of possible rulemaking for core-melt accidents.

While we do not believe that these developments at the NRC are the result of this work, these trends are clearly in the direction suggested here. Consequently, this report does not now offer any particularly unique or innovative recommendations. It does, however, in our opinion, summarize the key issues associated with attempts to develop regulatory modifications to address core-melt accidents.

1.0 INTRODUCTION

The Nuclear Regulatory Commission (NRC) is considering the promulgation of new regulations concerning core-melt accidents (CMAs). An Advance Notice of Proposed Rulemaking, which addresses both degraded and melted cores,* has already been issued.[1] The notice invites comments on 18 questions, which can be summarized as follows:

- Can degraded-core accidents (DCAs) be mitigated, and should they be considered as design-basis accidents in the safety analyses?
- Should CMAs be considered as design-basis accidents?
- What limits should be placed on multiple error and operator failure assumptions in safety analyses?
- What additional features, such as filtered venting of containment, improved hydrogen control systems, core retention devices, and self-contained decay heat removal systems, should be required? Can probabilistic risk assessment be used to determine the need for such features?

These questions seem to focus on two basic topics: (1) measures to protect against (i.e., prevent or mitigate) CMAs and (2) regulatory strategies for addressing CMAs. This report will provide the NRC with broad overviews of these two topics as a means to address the central issue of this study: the regulatory impact of including CMAs in the regulatory process.

The balance of this report examines each of these two areas of regulatory concern. Technical concepts for prevention or mitigation of CMAs are reviewed; then regulatory "strategies" or means by which various requirements have been included in the regulatory base are presented. The interaction between these, which characterizes the range of possible impacts on NRC regulations of corresponding CMA protection, is the final topic covered by this report. These sections are introduced more completely below.

---

*A previous report (see Reference No. 2) discussed the effects of degraded-core accidents (DCAs) on NRC regulations. A DCA and a CMA are distinguished by the fact that in a DCA, the core material would remain within the reactor pressure vessel.

Section 2.0 presents a brief overview of various concepts that have been proposed for preventing or mitigating CMAs. The section begins with a description of a CMA, an understanding of which is necessary in order to recognize the specific purpose of each proposed concept. A CMA is a complicated, incompletely understood event, although studies are underway to improve this understanding. There are many different accident sequences that can lead to a CMA, and the consequences of such an accident would vary, depending on the numerous possible operator and mitigating system responses. Therefore, it is difficult to assess how well a particular concept will prevent or mitigate a CMA. Figure 2-1 presents one way to logically organize the various proposed concepts. It is not necessarily a complete identification, and several concepts contribute to more than a single goal. However, it shows the role that each concept might play in meeting the overall objective of protecting against a CMA.

Section 3.0 examines ways in which various specific protective measures have been included in the regulatory base. A review of 10 CFR 50, 10 CFR 100, 10 CFR 20, and the NRC Division 1 Regulatory Guides was conducted to identify the various regulatory "strategies" that are currently used within the regulations and Regulatory Guides. Not all, however, are used for all sections of the regulations. Therefore, there is a choice to be made regarding the strategies by which different protective mechanisms for a CMA would be bound to the regulations.

Since the Three Mile Island Unit 2 accident, questions like the following have been raised:

- Is defense-in-depth adequate, or is another line of defense needed?
- Should safety analyses go beyond the current design basis to include CMAs?
- Should nuclear power plants be designed against multiple failures?

All of these questions can be combined into one question: "Are the current regulatory strategies adequate for protecting against CMAs?" Without attempting to answer this question, Section 4.0 provides a basis for core-melt rulemaking in terms of the protective mechanisms and strategies introduced in Sections 2.0 and 3.0, if it is determined that current safety practice and regulation for light-water reactors do not provide adequate protection.

2.0 ALTERNATIVE APPROACHES FOR IMPROVED PROTECTION AGAINST CORE-MELT ACCIDENTS

This section describes core-melt accidents (CMAs) and summarizes a range of protective measures for possible reduction of their risk. "Protective measure" refers, in this report, to any system, technique, or process designed to prevent or to mitigate CMAs. (See Figure 2-1.)

"Prevention" and "mitigation" are concepts definable relative to a given accident. Prevention of a CMA, for instance, may be accomplished by mitigating the effects of a degraded-core accident (DCA) sufficiently to preclude progression to a CMA. In general, this report defines prevention of a given accident as the act of terminating the event sequence at any point prior to the occurrence of that accident. Mitigation of a given accident is any act intended to intercede during the portion of the event sequence following the specified accident, in an attempt to reduce its ultimate consequences. Thus, in effect, each complete accident sequence defines a hierarchy of potential events occurring over time. Whether a mechanism prevents or mitigates an accident depends on where attention is focused along that event sequence. (See Figure 2-2.)

For instance, many current reactor safety features and regulations focus on preventing more than a small amount of core damage in any serious design-basis accident. A limited capability has been provided to mitigate this extent of damage to the core (e.g., hydrogen control systems as required before the accident at TMI-2).

Since a loss-of-coolant accident (LOCA) is one of the major events that could precede core damage, mitigating a LOCA through the use of an emergency core cooling system (ECCS) is one approach to preventing core damage.

Two important items unspecified in Figure 2-2 are (1) the precise points of interface between types of accidents and (2) other lines representing alternative accident evolutions. For instance, it is not clear that an imperfectly mitigated large break LOCA is necessarily a DCA; this depends on how a DCA is ultimately and precisely defined.[2] Similarly, it is apparent that a design-basis LOCA is not the only path to a DCA. In the case of a CMA and a DCA, the situation is somewhat more clear cut because they have been defined generically in this and preceeding reports.[2] In particular:

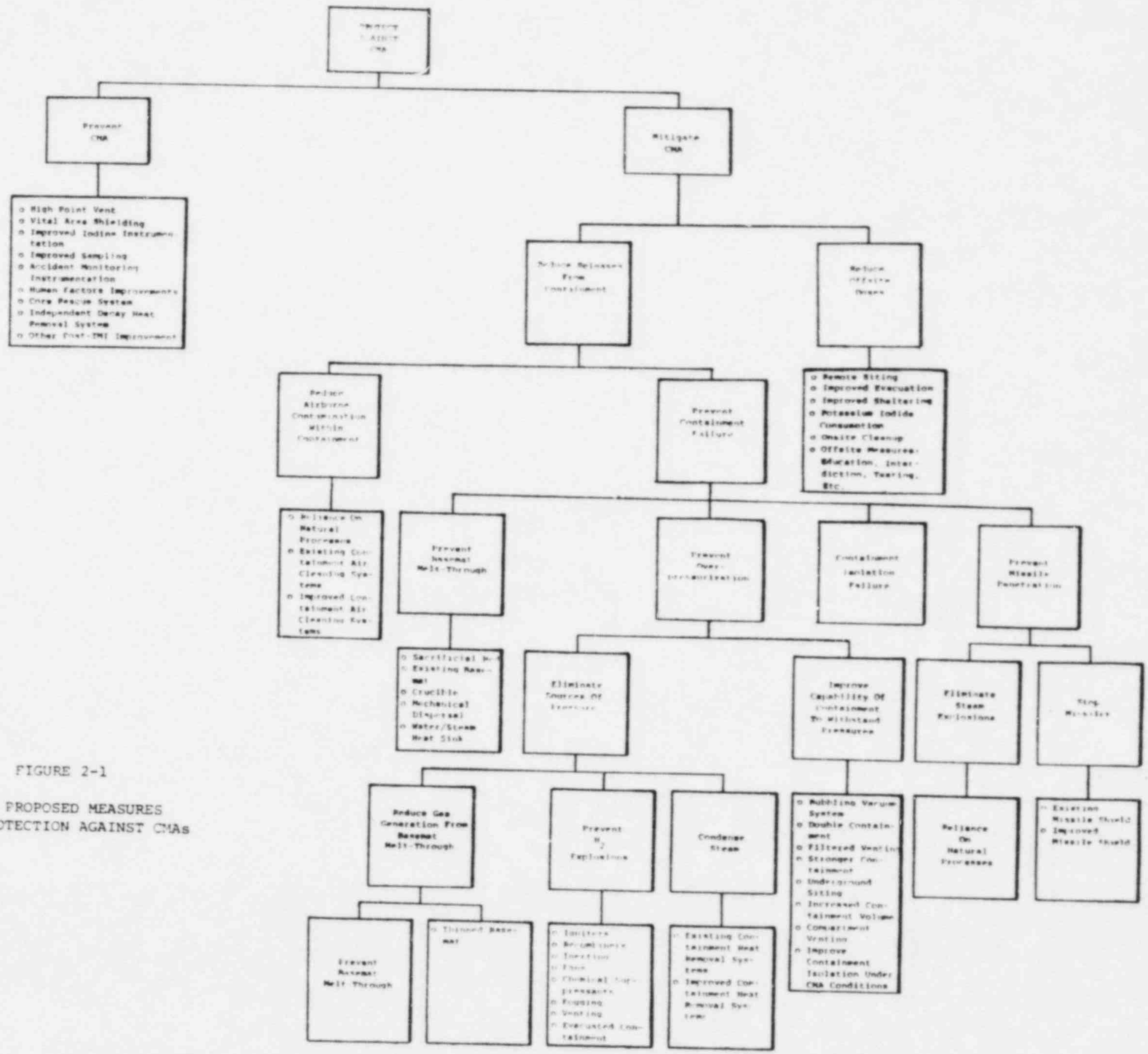
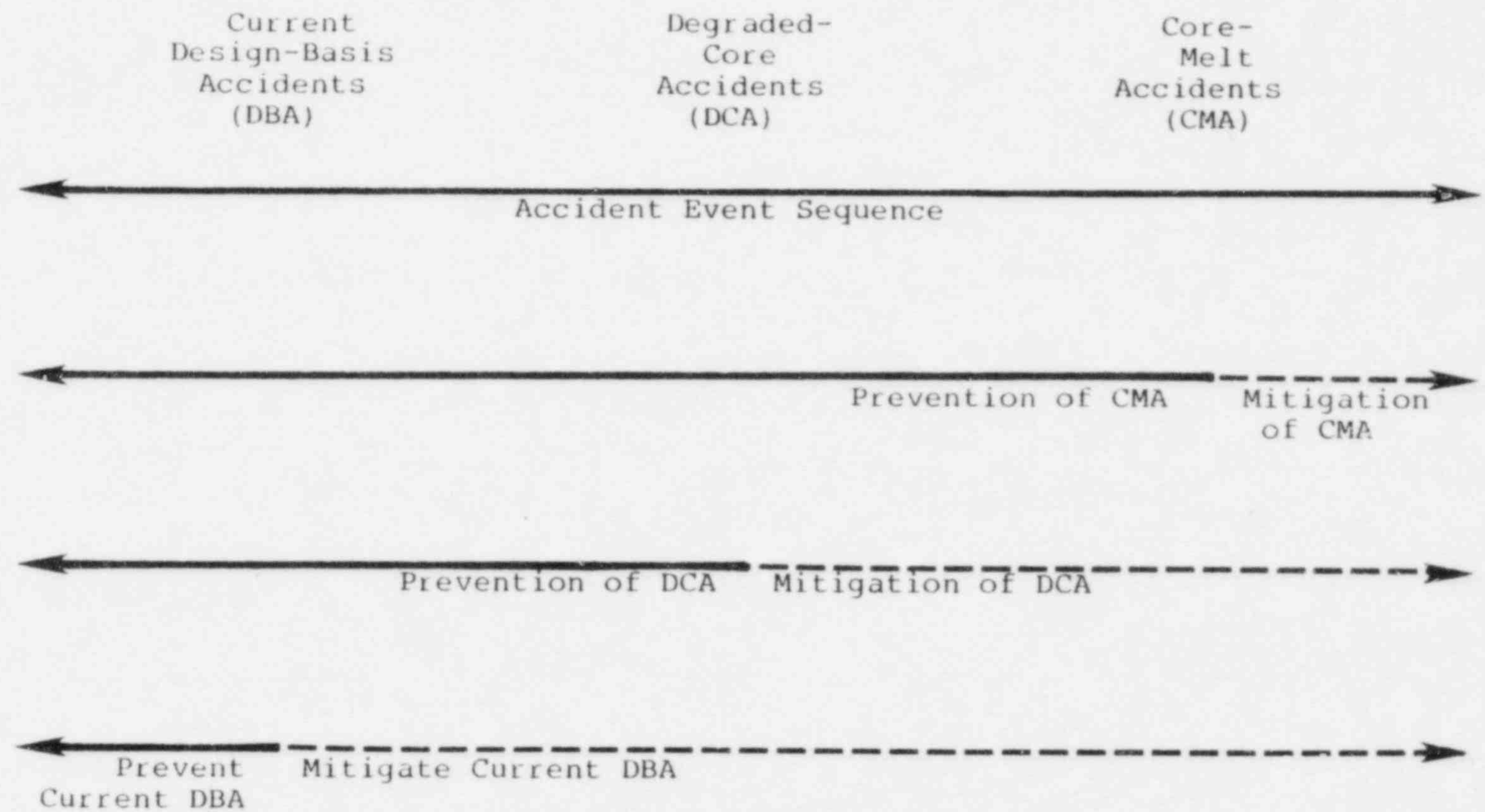


FIGURE 2-1

SOME PROPOSED MEASURES
FOR PROTECTION AGAINST CMAs

FIGURE 2-2

PREVENTION VS. MITIGATION IN AN ACCIDENT EVENT SEQUENCE



- Any accident that evolves from, but which exceeds, a DCA will necessarily be a CMA. This is a result of the general definition of DCA in a previous report,[2] which addressed the regulatory impact if DCAs were included in the regulations. These were defined as accidents that damaged the core, but for which the core was retained in the intact reactor pressure vessel.

- In most cases, a DCA will precede a CMA.

Exceptions to the latter would be accidents in which catastrophic pressure vessel failure precedes serious core damage. This could conceivably be the result of earthquake damage, missile damage, serious prior reactor vessel cracking followed by a transient inducing severe thermal shock, etc. These events are included within the definition of CMAs provided in Section 2.1, since it would be expected that, once the reactor vessel was severely breached (to an extent significantly greater than a large break LOCA), then the core might not be prevented from melting by existing safety systems. This type of reactor vessel failure is also beyond the current design basis.

Thus, any measure designed to prevent a DCA (i.e., current safety systems), or to mitigate a DCA,[2] may be viewed as a means to help prevent a CMA. Mitigation of a CMA is an attempt to prevent consequences to the public, given that an accident has occurred in which the reactor vessel has been breached.

2.1 DESCRIPTION OF A CMA

For the purpose of this report, a CMA is defined as a meltdown of the UO_2 fuel and core structural components, with subsequent melt-through of the reactor vessel. A catastrophic reactor vessel failure (not caused by melting) that causes the core to drop out of the reactor vessel can also be considered a CMA. This section will not deal with the numerous accident sequences leading to a core meltdown, but will very briefly describe, in a qualitative manner, the CMA phenomena and its possible consequences as an aid to understanding possible CMA prevention and mitigation concepts. The description will treat separately (1) the melt sequence leading to reactor vessel failure and (2) the possible containment failure modes.

2.1.1 CMA Events Leading To Reactor Vessel Failure

A CMA in a pressurized water reactor (PWR) could result from any of a large class of transients that lead to the loss of primary and/or secondary cooling, together with the loss of emergency core cooling, resulting in boiloff of the primary coolant. Uncovering of the fuel rods would cause them to overheat, leading to cladding rupture and oxidation, and eventually to the fuel melting. The following discussion describes the subsequent course of events that would be expected for a typical PWR, based on the "Report of the Zion/Indian Point Study."[3]

In Figure 2-3, a substantial fraction of the core is shown as having been exposed because of the low water level, in a coherent mass of core-melt material has formed above the water level, separated from it by successive layers of crust, sintered rubble, ZrO_2, fractured fuel, and intact fuel pins. Further up the core, a fraction of the steam flow has been converted to hydrogen flow by the reaction of the zircaloy cladding with the steam. When all of the water in the core has boiled away, the steam flow (and Zr/H_2O reaction) becomes negligible because the water is no longer heated directly by contact with the fuel. At this point, the water level is slightly below the lower core plate. Depending partially on the duration of this phase, the amount of coherent molten material could increase considerably; alternatively, molten material could flow downward in a narrow streaming fashion and and contact the water, resulting in an increased boiloff rate and melt-water interactions.

If the core-melt material remains as a coherent mass, a situation evolves in which gradual boiling of the water layers between the below-core structures exposes the lower core and diffuser plates, which subsequently weaken as they are heated to higher temperatures by the fuel rods above. The upper portion of the core barrel is uncovered early in the boiloff sequence and, thus, can be expected to attain substantially higher temperatures than would the below-core structures.

If the core barrel becomes so hot that it weakens and fails, a substantial portion of the ~150 tons of core and structure above could plunge downward several feet, coming to rest on the bottom of the reactor vessel. This downward relocation of the core would displace water, produce vigorous boiling, and perhaps induce a steam explosion by plunging hot core material into the water.

The location and size of reactor vessel failure, and the rate at which molten fuel pours from the vessel, would depend on the event sequence. For instance, in a failure occurring under primary system pressure, the molten core could pour from the vessel rapidly, under pressure. In a system depressurized due to a LOCA, the molten core pouring from a local failure of the vessel might be slow due to gravity. If fuel is not in contact with the bottom part of the vessel, then the remaining water would keep that portion of the vessel cooler than the top. In that case, local failure above the bottom of the vessel might result. If hot debris is in direct contact with the bottom of the vessel, then melting and plastic deformation of the entire bottom portion of the vessel might occur.[4] (See Figure 2-4.)

FIGURE 2-3

GENERAL STRUCTURE AND FEATURES OF MELTDOWN IN A TYPICAL PWR REACTOR VESSEL[3]

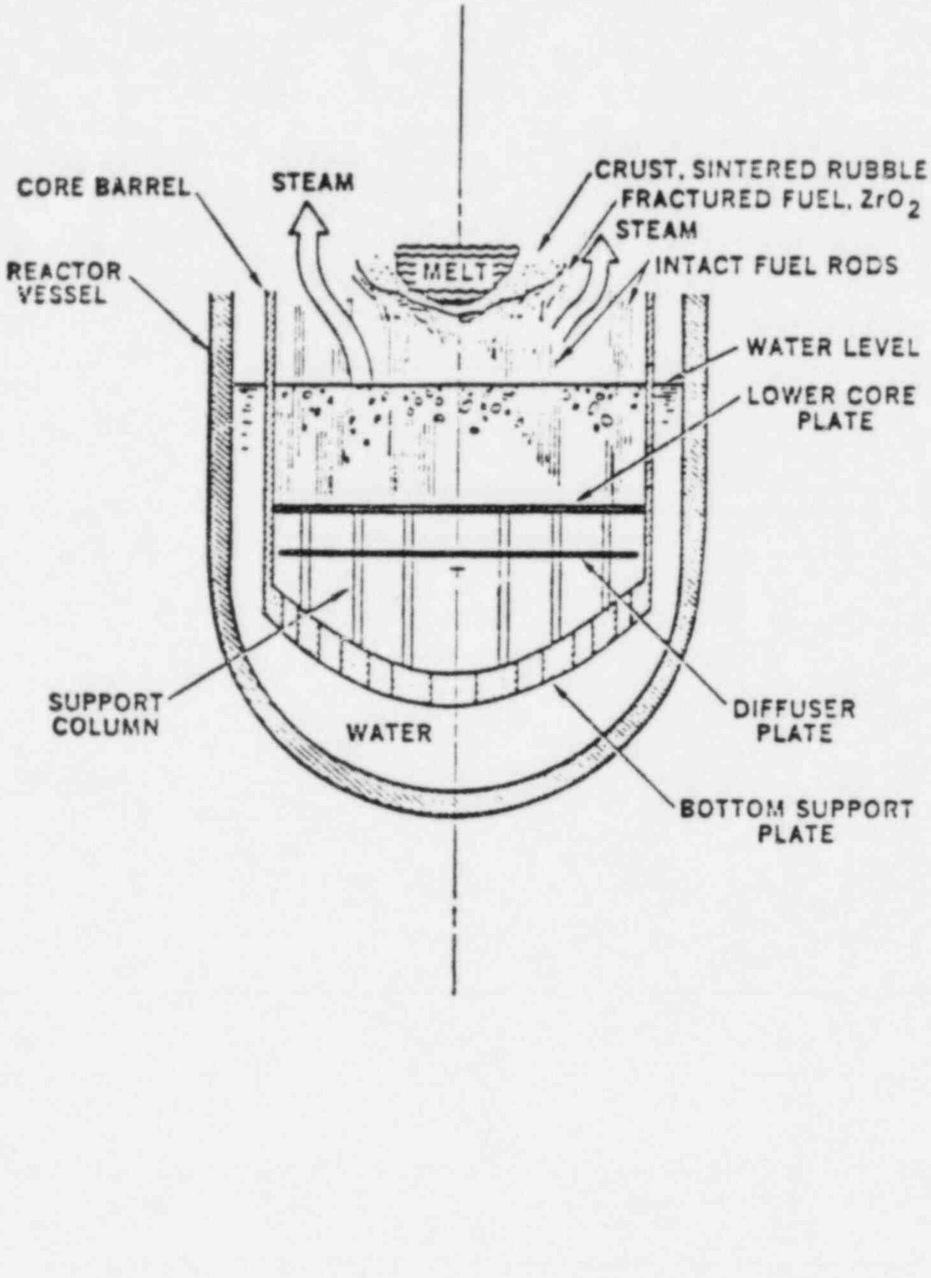
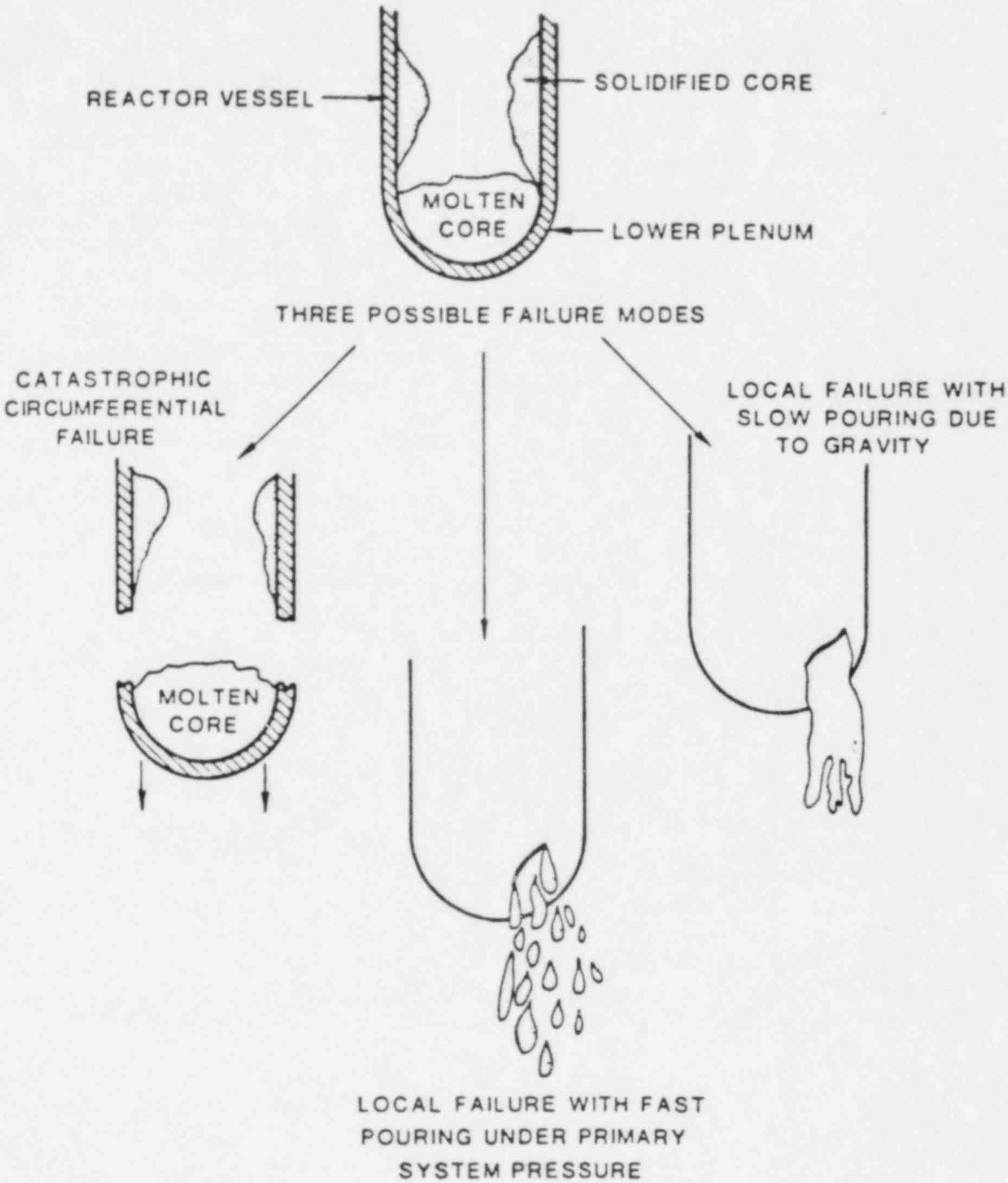


FIGURE 2-4

VARIOUS POSSIBLE MODES
OF LOWER-PLENUM FAILURE[4]



Although the details of the accident sequence up to reactor vessel failure will depend on initiating events and reactor design (in particular, pressurized water reactor [PWR] vs. boiling water reactor [BWR]), the above description portrays the major elements pertinent to the scope of this report. The uncertainty regarding precise phenomenology needs also to be kept in mind, so that the most detailed accounts are, of necessity, the most speculative.

2.1.2 Containment Failure Modes

Given that a CMA has occurred, the consequences to be expected will depend largely on the degree, mode, and phenomenology of containment failure and subsequent releases to the environment. There are a number of containment failure modes associated with a CMA, both while the core is still inside the reactor vessel and after it has penetrated the reactor vessel. Primarily, the containment may fail because of overpressurization, basemat melt-through, missile penetration, or failure of containment isolation. (See Figure 2-1.) Direct failure (e.g., due to an earthquake) is not considered since it would not result from a CMA in particular. If CMA protection were to be included in the regulations, however, a decision would be required to determine whether a CMA and containment failure resulting from a common initiating event such as an earthquake should require protection. The failure modes and their causes are interrelated, as discussed in the following subsections.

2.1.2.1 Steam Explosions. In the event of a CMA, molten fuel would drop into the remaining water in the reactor vessel lower plenum. If a major fraction of the core is molten (5%-20%) and becomes submerged in the water, a steam explosion could result. An explosion could result, further, in reactor vessel failure due to a shock wave or a liquid slug impacting the upper head. A possible consequence of this interaction would be the generation of solid missiles from the reactor vessel, which might threaten containment integrity.[3] As is true in the rest of the accident description, various details of design and accident progression could mitigate the events to a greater or lesser extent.

The possibility of an ex-vessel steam explosion exists if the molten core, or corium falls into the water in the reactor vessel cavity. A water slug from the explosion would have to travel up through the failed reactor vessel lower head, into the reactor vessel, and then follow the same path that it would follow for an in-vessel steam explosion. Internal structures and equipment shield the containment shell from missiles originating from such steam explosions.

In general, the above discussion of in-vessel steam explosions can be applied to BWRs as well as to PWRs. However, depending on the specific accident sequence in a BWR, there may be no water remaining in the reactor vessel when the core melts.

There is also the possibility of an ex-vessel steam explosion if the corium falls into water on the drywell floor. The configuration of the drywell to wetwell vents could permit some water to remain on the drywell floor. The temperature of this water could range from subcooled to saturated, depending on the particular accident sequence. If the molten materials were to fall into the water in relatively small quantities and over a period of time, they would simply be quenched, and the steam generated in the process would be condensed in the suppression pool. If, on the other hand, a significant fraction of the core were to fall into the water coherently, there would be the potential for a violent interaction. Such a violent interaction has the potential to fail the containment, if it occurs when the containment is still intact.[5]

2.1.2.2 Combustible-Gas Effects. During a CMA in a PWR, hydrogen is produced as a result of the zirconium-steam reaction, steel-steam reaction, radiolytic decomposition of water, and decomposition of zinc-based paints and coatings. The primary source of hydrogen during the early phases of a CMA is the zirconium-steam reaction, which could theoretically produce enough hydrogen to cause a hydrogen burn that could exceed the design pressure in some containments.[6] Later, during a CMA, the corium/concrete interaction can produce a quantity of combustible gases (hydrogen, carbon monoxide, and perhaps methane) of the same order of magnitude as the metal-steam reaction. The combustible gases produced during a CMA mix with the containment atmosphere, which, in addition to air, would also contain carbon dioxide, steam, and fission-product gases.

The potential for containment rupture due to hydrogen burning depends on a number of factors:

- Composition of the atmosphere;
- Availability of an ignition source; and
- Incremental pressure rise associated with burning.

At a temperature below about 650°F, hydrogen and air can ordinarily be mixed in any ratio without observable chemical reaction. However, these mixtures can burn rapidly if an ignition source, such as an electric spark, exists. The combustion can be (1) a deflagration, in which the flames travel at subsonic speeds, or (2) a detonation, in which the flames travel supersonically and produce shock waves. The pressure rise resulting from deflagration is slow, and the containment responds only to the magnitude of the pressure with no dynamic effects. Detonation causes intense shock pressures of short duration in the containment, followed by a residual pressure equal to that of the slow deflagration. Because of the short duration of the intense shock pressure, the damage caused might not be as severe as a steady pressure of the same magnitude.[6] The potential for combustion, and for detonation if combustion occurs, depends on the composition of the gases present.

The probability that failure of containment would occur due to combustion depends on a number of factors, including the pressure increase that it induces, compared with nominal failure levels. This, in turn, may depend on: containment volume (e.g., ice condenser PWRs appear to be more vulnerable to damage from combustion due to their smaller free volume); containment design pressures; static pressure at the time of combustion (which might be susceptible to manipulation by accident mitigation mechanisms); etc.

Most BWR containment atmospheres are inerted by purging with nitrogen until the oxygen content is below 5%. The oxygen is maintained at or below this level during normal operation. At this oxygen concentration, the containment atmosphere is outside hydrogen flammability limits, regardless of the amount of hydrogen in the atmosphere. Radiolytic decomposition of water during the course of the accident would add oxygen as well as hydrogen to the atmosphere. During the early stages of the accident, radiolytic decomposition of water would not result in a flammable mixture. For longer time periods than about one day, the containment might have failed by other mechanisms, and in that case hydrogen combustion would not be a concern.[5]

2.1.2.3 Basemat Melt-Through. Basemat melt-through is another possible containment failure mode. A number of variables could influence the degree of basemat penetration by a molten core. The mode of reactor vessel failure is one of the variables. The molten core could do the following: (1) drop down all at once, together with the lower portion of the reactor vessel; (2) pour out slowly by gravity from a local failure in the reactor vessel; or (3) pour out quickly under primary system pressure from a local failure in the reactor vessel. Which mode occurs would affect the way in which the corium initially spreads out and fragments on the floor of the basemat. The amount of fragmentation and spreading would determine the amount of surface area available for removal of heat generated in the corium. The geometry of the structures below the reactor, which is plant specific, would also affect the way in which the corium initially fragments and spreads out.

Depending on the exact accident sequence, a pool of water could be present on the floor when the corium falls out of the reactor vessel and could cause the corium to fragment. Also, the water would remove heat by natural convection and steam production.

Assuming that no water is present to cool the corium, or that the corium is not fragmented enough to be cooled by water, the corium would begin to penetrate the concrete basemat. The extent of penetration would depend on a number of factors, including the heat generation rate, the surface area of the melt, and the amount of heat transferred up into the containment building, rather than into the concrete basemat.[4] These factors will vary with the facility and the accident sequence itself. For instance, initial decay heat rate may vary, depending on the time between reactor shutdown and vessel failure.

To date, experimental and analytical investigations have not resolved the roles and behavior of these factors sufficiently to predict whether the basemat would be penetrated during a CMA.

2.1.2.4 Containment Overpressurization. Failure of the containment by overpressurization can occur due to a buildup of pressure in the containment from the production of steam, hydrogen, carbon dioxide, and other gases. Unless the steam is condensed by containment heat removal or unless the containment is vented, containment failure could result. The failure could occur before or after reactor vessel melt-through, depending on the accident scenario and the reactor type.

In addition to static load, sizeable pressure spikes could occur in a PWR during a CMA sequence due to the following phenomena:

- Steam release from the primary system to the containment when the reactor vessel fails at high pressure;
- Rapid steam formation caused by the molten core's interaction with water existing in the cavity at the time of reactor vessel failure;
- Rapid steam formation caused by the flashing of some of the residual water in the primary loops when the reactor vessel fails, and by the dumping of the remainder of this residual water onto the molten core that is in the cavity;
- Rapid steam formation caused by the discharge of accumulated water at the time of reactor vessel failure and interactions of this water with the molten core in the cavity;
- Deflagration of the hydrogen produced by zircaloy-steam reaction, triggered by the interaction of the molten core with the concrete in the cavity; or
- Production of steam and noncondensible gases resulting from the interaction of the molten core with the concrete in the cavity.[7]

A primary difference between the risk-dominating accidents in the BWR and in the PWR is that those in the BWR involve containment overpressurization before the core begins to melt. For those accidents in which meltdown precedes containment overpressurization, a pressure spike is predicted to occur when the reactor vessel fails, with the following phenomena responsible:

- Hydrogen release from the primary system to the containment if the reactor vessel fails at high pressure; and

- Rapid hydrogen production caused by molten zirconium interaction with water existing on the drywell floor at the time of reactor vessel failure. No hydrogen burning takes place due to an inerted containment in most BWRs.

The primary source of the pressure spike in the BWR, with its smaller primary containment, is hydrogen, rather than steam. However, a fairly sizeable pressure spike might also occur if the suppression pool were saturated.[7]

2.1.2.5 Containment Isolation Failure. Each line that connects directly to the containment atmosphere and penetrates the primary reactor containment must be provided with isolation valves inside and outside of the containment as required by 10 CFR 50. These valves preserve containment isolation by preventing the release of radionuclides in the form of noncombustible gas, steam, or aerosols. They can be actuated manually or automatically, so a possible loss of containment isolation could occur due to human or automatic system failure.

2.2 APPROACHES TO PREVENT A CMA

Recent literature on CMAs has focused more on mitigation than on prevention. Some possible reasons for this are noted in Section 2.3. However, there are a number of approaches for protecting against a CMA that involve additional systems, procedures, or training to prevent an accident from degenerating into a CMA.

As stated previously, a reactor core could be in a degraded state for some time before a CMA occurred. Therefore, any measure intended to prevent a DCA and some intended to mitigate a DCA can also be considered as an approach for preventing a CMA. In fact, existing safety systems at nuclear power plants are intended to prevent CMAs. Many new approaches have been proposed since the TMI-2 DCA. Summaries of some of these new approaches are included below.

2.2.1 High-Point Vent

The high-point vent is intended to allow venting of noncondensible gases (e.g., hydrogen) that may accumulate in the primary reactor coolant system during a DCA.[8] Unless removed, these noncondensibles might impair natural circulation or main coolant pump operation and, thereby, might contribute to a CMA.

2.2.2 Vital Area Shielding

Certain vital areas to which access may be required during a DCA could experience high radiation levels. Additional shielding has been proposed so that personnel can access these areas to perform vital functions intended to prevent the DCA from becoming a CMA.[8]

2.2.3 Improved Iodine Instrumentation

Improvements for existing instrumentation are planned. Current instrumentation may overestimate the airborne radioiodine concentration, so that plant personnel may be needlessly required to wear protective respiratory equipment. Such equipment can limit communications ability and diminish personnel performance during an accident.[8]

2.2.4 Improved Sampling

The ability to quickly analyze reactor coolant and containment air samples allows better assessment of system conditions during an accident. The Nuclear Regulatory Commission (NRC) has proposed requiring the capability to promptly analyze samples to determine the quantity of radioisotopes in the primary coolant; hydrogen in the containment atmosphere; and dissolved gases (total and hydrogen), boron, and chloride in the primary coolant.[8] Such information might be important in preventing a DCA from becoming a CMA.

2.2.5 Accident-Monitoring Instrumentation

New instrumentation has been proposed to give the operator information to follow the course of an accident and, in particular, to detect inadequate core cooling. Variables to be monitored include containment pressure, containment hydrogen concentration, containment water level, reactor water level, containment radiation level, and primary coolant subcooling.[8]

2.2.6 Human Factors

A number of proposals have been made to improve operator response to an accident. These include improved control panel design, more simulator training, and additional personnel (e.g., a Shift Technical Advisor). Such improvements might help operators prevent a CMA.

2.2.7 Core Rescue System

In a paper presented at the International Atomic Energy Agency (IAEA) Conference on Current Nuclear Power Plant Safety Issues, Petrangeli cautions against rushing into engineering efforts directed at the design and construction of devices for mitigating a CMA.[9] His caution is based on his belief that the large uncertainties surrounding the consequences of a CMA would necessitate a large, time-consuming research and development (R&D) effort before a phenomenological basis could be provided to allow engineers to responsibly design such mitigating devices. As an alternative, he proposes the Core Rescue System (CRS), which is intended to prevent a CMA from occurring. The CRS includes in-core temperature instrumentation, in-core neutron flux instrumentation, core water-level instrumentation, an emergency coolant injection system, a SCRAM system, an automatic pump trip (BWR only), a liquid poison injection system, and a coolant exit port (i.e., relief and safety valves). Some of this equipment already exists in most reactors and could be incorporated into the CRS. The control room would contain a "core-in-danger" alarm, as well as controls for the emergency coolant injection and SCRAM systems. In the event of a core-in-danger alarm, the CRS procedure would take precedence over any other emergency procedures.

2.2.8 Improvements In Decay Heat Removal Systems

Improving decay heat removal reliability (i.e., reliability of the auxiliary feedwater system [AFWS], the residual heat removal systems [RHRS], and/or the high-pressure service-water systems [HPSWS]) could significantly reduce the probability of a CMA in some light-water reactors (LWRs).[10] One way to improve the reliability is by adding another independent train for decay heat removal. The NRC is addressing shutdown decay heat removal requirements as an unresolved safety issue. It plans to investigate alternative PWR decay heat removal methods (other than those normally associated with the steam generator and secondary system), as well as means for improving the reliability of decay heat removal systems in BWRs.

2.3 APPROACHES TO MITIGATE A CMA

Mitigation measures are the protective features most associated with possible CMA rulemaking. To some extent, this may be due to the perception that mitigation is a new approach to safety. In fact, as indicated previously, it is not; many existing safety systems mitigate the effect of a transient. Nuclear reactor regulatory philosophy for the past several years, however, has focused on preventing core damage and assuming that such prevention is sufficient protection against a CMA. Thus, mitigation of accidents that severely damage (or melt) the reactor's core is relatively new.

Another factor involved in the current interest in CMA mitigation may be the perception that it provides blanket protection against any eventuality not covered by other means. Review of the literature, as summarized below, does not support this perception. The efficacy of CMA mitigation schemes is not guaranteed or complete. As is the case with other engineered safety systems, the effectiveness of these systems depends on the conditions under which they actually operate, compared to design conditions, operator response, etc. Many of these conditions depend on the accident sequence leading to core melt and are not completely known at this time. Thus, any design of these measures must be based, at least in part, on well-founded assumptions, which can be as controversial as any assumptions made with regard to current safety sytems. Even in cases for which phenomena are better understood, the inability to guarantee successful mitigation under all circumstances requires design choices and tradeoffs, just as do other engineered systems. In some cases, implementation of a particular mitigating system may influence the probability of success of other means of mitigation due to systems interactions that are not always favorable.

Two basic approaches exist for mitigating a CMA. These are (a) reduction of the radiological releases from containment, and (b) reduction of offsite doses given containment failure. The first approach may be accomplished by preventing containment failure or reducing the airborne contamination within containment. Each of these approaches is discussed below.*

2.3.1 Reduction Of Radiological Releases From The Containment

Most of the effort specific to CMA protection has been devoted to the reduction of releases from the containment, given that a core melt has occurred. The two major means for accomplishing this goal would be by reducing airborne contamination within the containment and by preventing containment failure. The latter could be achieved by preventing any of the major modes of containment failure, as discussed in Section 2.1.2. These modes include basemat melt-through, overpressurization, and missile penetration. In particular, there are several ways to reduce the probability of containment failure by overpressurization, including improving the capability of the containment to withstand the sources of pressure in a CMA and eliminating the sources of pressure themselves. (See Figure 2-1.) These topics are reviewed briefly below.

2.3.1.1 Prevention Of Containment Failure. At least eight alternative containment designs have been suggested for reducing the probability of containment failure due to overpressurization during a CMA. These designs** are stronger containment, shallow underground siting, deep underground siting, increased containment volume, filtered atmospheric venting, compartment venting, double containment, and bubbling vacuum system.

During a CMA, the danger of a containment breach from high pressure comes from sources within the primary system or the containment. The high pressure is caused mainly by the generation of hydrogen, steam, or other noncondensibles from the chemical reactions that occur during a CMA. The amount of gases generated depends on the individual accident scenario. Rather than designing the containment to withstand such pressure, another approach is to eliminate the sources of the pressure.

Gases may be released to, or generated within, the containment from several sources. As described in Section 2.1, these gases include hydrogen, oxygen, carbon monoxide, carbon dioxide, methane, and gaseous fission products. In addition, steam formation contributes

---

*Additional detail may be found in the literature. Refer to the Reference List on page R-1.

**The literature describes these designs [7,11,12,13] and, in some cases, compares their effectiveness in reducing risks from a CMA.

to pressure increase. Major sources of such gases include metal-water reactions and concrete-melt interactions, with additional contributions from corrosion and radiolysis.[6]

The removal of hydrogen, in particular, is considered to be of paramount importance, as it presents a threat to both the primary system and the containment. In the primary system, it could accumulate at high points and interfere with natural circulation. In the containment, hydrogen largely contributes to the buildup of high pressure and presents a potential source of deflagrations or detonations, which in turn could cause pressure spikes exceeding the design pressures of the containment.

Hydrogen control, which is the prevention or mitigation of the detrimental effects of hydrogen, is under study, and several concepts are being investigated. Measures that already exist in the effort to control hydrogen and some new schemes include: inerting of the containment; flaring; use of fans to disperse locally high concentrations of gas; use of recombiners; use of fire suppressants; fogging; and operation of the containment at reduced pressure, normally thereby reducing the partial pressure of oxygen and reducing the likelihood of ignition.[3,6-8,14] The use of these, as well as other engineered safety features such as purge systems or filtered venting systems, is being considered for hydrogen control.

The generation of high pressure from steam could also cause overpressurization of the containment during a CMA. Current regulations require heat removal systems such as a containment spray injection system, a containment spray recirculation system, and a containment heat removal system, which are designed for a LOCA. The amount and rate of steam generation during a CMA might exceed the capacity of these systems. There are heat sources other than core decay heat during a CMA, such as zirconium-steam reactions and corium-basemat reactions. Therefore, expansion or upgrading of current systems is one method that can help in steam control. Steam explosion is another factor considered to be a possible threat to the containment.[3]

Another contributor to the increase in containment pressure is the generation of noncondensible gases in the melted-core/concrete-basemat interaction. Concepts to prevent the core-melt from coming into contact with the concrete would eliminate some of these noncondensible gases, as well as prevent basemat melt-through. Some of the concepts include the use of: a water/steam heat sink, along with filtered venting; a sacrificial bed of specially chosen material; a sacrificial material as a crucible; a structure to disperse the molten core to improve heat transfer from it; and a thinner basemat to reduce gas formation from melt-through.[7] Clearly, each of these concepts must be evaluated properly for feasibility, risk reduction potential, cost, and interaction with other requirements for CMA mitigation.

During a CMA, another mode of containment failure, in addition to overpressurization, results from basemat melt-through. The result would be a release of radioactive materials into the soil beneath the reactor building. This action could pose a health hazard to the public if the material were subsequently to contact groundwater or to migrate to the ground surface. Therefore, one approach to mitigating some CMAs is to prevent basemat melt-through. (However, if heat that does not go into melting the basemat is rejected into the containment, it could accentuate containment overpressurization.)

To prevent basemat melt-through, heat must be transferred from the corium fast enough that the concrete temperature falls below the disintegration temperature before the corium penetrates to the outside surface of the basemat. Various ways to prevent melt-through have been suggested in the literature. These methods include the use of: a sacrificial bed, or crucible; a water/steam heat sink; and mass dispersal devices.[4,15]

The concrete basemat of a typical LWR plant might be able to prevent basemat melt-through by itself. A number of analytical and experimental studies have been done to determine the degree of corium penetration into concrete. However, too many uncertainties remain for investigators to predict conclusively whether a typical concrete basemat can arrest penetration.

Even if basemat penetration occurred, groundwater contamination would not necessarily follow. Such contamination would depend on the location of the water table and the permeability of the soil under the basemat. For example, in a study done for the President's Commission on the Accident at Three Mile Island, it was noted that the TMI-2 containment is built on red siltstone bedrock, which is not penetrable by water.[16] This is another area in which improved phenomenological insight may influence the form or degree of eventual CMA requirements.

2.3.1.2 Reduction Of Airborne Contamination Within The Containment. While prevention and control of high pressures generated within the containment during a CMA are important, the ultimate goal of onsite mitigation is to limit the release of radiation into the environment. If the quantity of fission products in the containment atmosphere were small, then the consequences of a containment failure would not be as severe as generally expected. Levenson and Rahn's study[11] points out that the natural conditions that would exist during a CMA might greatly help in reducing the amount of radionuclides released into the air, even if the containment were breached. The study points out several natural processes that would help retain the radionuclides within the containment. They include: factors favoring agglomeration of aerosols and settling of the resultant particulates; trapping of the particulates in cracks; immobilization of volatiles in water; plating out of fission products; and reaction of radioiodine with substances inside of the containment, leading to immobilization of that material.

Such factors create natural barriers to the escaping airborne radionuclides. Additionally, systems such as the containment sprays with chemical additives could be used to absorb and retain fission products within the containment. The phenomenological understanding of these natural mechanisms is incomplete. Quantification of the reduction in estimated consequences due to these factors may reduce the need to add additional systems for CMA protection. Whether these phenomena reduce the need for CMA protection depends not only on the degree of protection they afford, but also on the strategy chosen for regulation. For instance, a risk-based strategy that gave credit for risk reduction due to such processes might favor reliance on natural processes more than a specific system strategy that assumed the need for a given system. (See Section 3.0.)

2.3.2 Reduction Of Offsite Doses Due To A CMA

The title of this section is somewhat of a misnomer, since the goal of all CMA mitigation is to reduce offsite doses. It is intended to refer to the mitigation of a containment failure with high levels of contamination in the containment. In effect, these measures are aimed at mitigation of the failure of the last onsite barrier to release. If additional engineered systems for CMA mitigation are installed onsite, then the measures described in this section mitigate their failure, thus proving that mitigation of a CMA is not necessarily the "last word" in safety! For the most part, this section refers to "emergency response" measures, but that should be understood to apply to techniques that may continue over long periods, such as testing of items in the food chain, interdiction of property, and education of the public, as well as short-term responses such as evacuation. The major thrust of these measures is the recognition that harm to the public health and safety depends largely on the dose received by individuals due to the accident, and that this may be positively influenced even after an offsite release.

CMAs can be grouped broadly into two major categories that affect emergency response characterization. In both categories, the important factors that govern emergency response are the time and duration of radioactive release, the type and quantity of radioactive release, and the distance between the reactor and the nearest population area. The first category involves containment failure by basemat melt-through. In the second category, breach of the containment occurs directly to the atmosphere.

The first type of failure (basemat melt-through) is characterized by a long (3-10 hours), continuous release of radionuclides that begins relatively long (10-30 hours) after the initiating event that led to the CMA, depending on the reactor type and the accident sequence.[5] Also, relatively small fractions of the radionuclides of the core inventory are released into the atmosphere. The second case (breach to the atmosphere) is generally of shorter

(0.5-4 hours) duration, during which possibly a large fraction of the core's radionuclide inventory may be released into the air. The release may begin as soon as 2-3 hours after the initiating event, although longer delays may occur prior to release. Again, these values depend on the reactor type and the accident sequence.

Given a CMA or the possibility of a CMA, the emergency response would be based on one or a combination of the following options:

- Evacuation;
- Shielding, with evacuation at a later time; and/or
- Blocking the thyroid's radioiodine uptake by the immediate ingestion of stable iodine.

The Environmental Protection Agency (EPA) has established Protective Action Guides (PAGs) for whole-body and thyroid exposure to accidental airborne releases. These limits are designed such that any dose received by the population below that limit would not result in any detectable early biological effect in the most sensitive population group. With these limits as guidelines, various options to try to prevent the population from being overexposed are available in case of a CMA. The best choice of emergency response would depend on the speed and quantity of radionuclide release, the delay between the time that protective action is undertaken and release begins, the population distribution near the plant, weather conditions, the availability of resources for emergency action, and the quality of implementation of emergency action by officials and the affected public. The estimated effectiveness of each option for emergency action is a source of controversy, as evidenced by varying treatments in the literature.[11,17,18] A major difficulty appears to be in the inability to estimate radiological consequences of a CMA with sufficient accuracy for planning emergency action. Current controversy over the effectiveness of natural removal processes (for radioiodine in particular) following a CMA may significantly affect a best-estimate model of consequences.[17] The uncertainty surrounding these models, and the difference between a best-estimate model and the usual conservative regulatory models may be significant in applying the results to emergency planning. In particular, the difficulty in accurately estimating consequences is significant due to the coupling between emergency action strategies and characteristics of the release, and because emergency action itself carries certain risks. (For instance, evacuation may result in accidents or in increased exposure under some circumstances.) In addition, there is the complication due to highly uncertain human factors influencing the effectiveness of emergency action. (For instance, the effectiveness of emergency evacuation could be compromised by evacuating larger areas of persons than required, thereby blocking evacuation routes and creating greater risk.) In all of the literature reviewed, the major estimated impact on public health appeared to be local (i.e., within approximately ten miles).[18] For this reason, siting at least ten miles from any concentration of population is proposed, by some, as a viable CMA mitigation measure.

3.0 CURRENTLY USED REGULATORY STRATEGIES

For the purposes of this report, a "regulatory strategy" is defined as the safety philosophy behind one or more requirements as stated in Nuclear Regulatory Commission (NRC) regulations. The overall purpose of the NRC's nuclear power plant regulations is to ensure that the operation of commercial nuclear power plants does not endanger public health and safety. The precise meaning of this phrase, and how to achieve the desired level of safety, are subject to various interpretations. It follows that there are numerous possible regulatory strategies.

The term "strategy" is used in this report to identify the different technical bases, within the regulations, that are used to make judgments on the safety of reactor plants. For example, "defense-in-depth" is often used to describe the current regulatory strategy, although the term is not explicitly defined in the regulations. The Advance Notice of Proposed Rulemaking on degraded or melted cores associates defense-in-depth with the requirement for "conservative design; multiple physical barriers; quality assurance for design, manufacture, and operation; and continued surveillance and testing to prevent [design-basis] accidents.[1] Solomon uses defense-in-depth to mean "multiple barriers (or mitigating devices)...used in the event of fission-product release from the fuel."[19]

Another term that has been used to describe the NRC regulatory strategy is "three layers of safety":

> Build plants right in the first place with good design and good materials; anticipate failures and provide safety systems to cope with those failures; assume that serious accidents happen and provide features to mitigate even these serious accidents.[11]

The NRC "Reactor Safety Study" states that the safety design strategy for nuclear power plants has been described in two ways:

- Three levels of safety involving (1) the design for safety in normal operation, providing tolerances for system malfunctions, (2) the assumption that incidents will nonetheless occur and the inclusion of safety systems to protect the public, and (3) the provisions of additional safety systems to protect the public based on the analysis of very unlikely accidents; and

- Physical barriers (fuel, fuel cladding, reactor coolant system, containment building) to attempt to prevent the release of radioactivity to the environment.[5]

Review of the NRC regulations indicated that a variety of regulatory strategies is actually used, such as risk, design-basis accidents, and single failure. Terms such as "defense-in-depth" and "three layers of safety," as defined above, are too general and simplistic to accurately describe all of the current regulatory strategies. In addition, the various strategies are rarely used independently of one another.

A brief review of 10 CFR 50, 10 CFR 20, 10 CFR 100, and the NRC Division 1 Regulatory Guides revealed that there are at least nine different regulatory strategies within the existing body of NRC nuclear power plant regulations. In many cases, they are implicit within those regulations. The following subsections define each strategy and give examples of specific regulations based on each.

3.1 COST-BENEFIT STRATEGY

In the cost-benefit strategy, additional safety equipment is required as long as the safety or health benefit of the equipment, measured in dollars, is greater than its cost. This strategy forms the basis of the as-low-as-reasonably-achievable (ALARA) regulations. NRC Regulation 10 CFR 50.34a requires that equipment to control radioactive effluents must be designed such that releases are "as low as reasonably achievable (ALARA)," taking into account the state of the technology and cost-benefit economics. Further clarification is provided in Appendix I of 10 CFR 50, which requires that the applicant must install all technologically available equipment that yields a favorable cost-benefit ratio, assuming a $1000 benefit for each man-rem reduced. Detailed calculational procedures that can be used to estimate the man-rem reductions and the equipment costs are given in Regulatory Guides 1.109 and 1.110. The ALARA regulations apply to routine radiological releases from normal plant operations. Regulations that address releases due to accidents are not based on the cost-benefit strategy.

3.2 ABSOLUTE-LIMIT STRATEGY

In the absolute-limit strategy, a quantifiable limit is imposed on an important measurable physical quantity. A regulation based on this strategy requires (1) that the plant be designed and operated such that the limit is not exceeded and (2) that specific actions be taken if the limit is exceeded. In some cases the limit may be related to a [illegible] value significant for safety. Sometimes it is based on what is believed to be a conservative margin on a value, based on a probability distribution. Other criteria exist as well. There are numerous examples of regulations based on this strategy.

Safety limits, which are part of the Technical Specifications required under 10 CFR 50.36, represent a good example of the absolute-limit strategy. Safety limits are those limits placed "upon important process variables which are found to be necessary to reasonably protect the integrity of certain of the physical barriers which guard against uncontrolled release of radioactivity." The regulation requires that the reactor be shut down if any safety limit is exceeded. The values for safety limits are based on the knowledge that damage to the plant could occur if the limits were exceeded. This knowledge is derived from analytical and/or experimental results. Achieving this limit is sufficient to bound the behavior of the reactor away from the damaging behavior, although it may not be known precisely what margin exists. An example of a safety limit is that the reactor coolant system pressure in a boiling water reactor (BWR), as measured in the reactor vessel steam dome, shall not exceed 1325 psig during power operation.

Another example of the absolute-limit strategy is contained in 10 CFR 50, Appendix G, "Fracture Toughness Requirements." Section IV B of this appendix requires that ferritic materials used to construct the reactor vessel beltline must have a minimum upper shelf energy, as determined by a Charpy V-notch test, of 75 ft-lbs. According to the NRC, below this limit the steel might not have adequate resistance to brittle fracture.

A third example of the absolute-limit strategy is the radiation exposure limit contained in 10 CFR 20.101, which prohibits a nuclear plant employee's whole-body exposure from exceeding 3 rems in one calendar quarter. Maintaining exposures below this limit is considered necessary to protect the health of the worker.

3.3 MULTIPLE-BARRIER STRATEGY

The multiple-barrier strategy states that a specific number of passive physical barriers must surround the radioactive material in order to prevent accidental release to the environment. In the NRC regulations, three barriers around the fuel pellets in the core are considered adequate. These barriers are the fuel cladding, the reactor coolant boundary, and the containment structure, as required by Section II of the General Design Criteria (Appendix A, 10 CFR 50). The reactor must be designed such that the design limits of the fuel cladding and the reactor coolant boundary are not exceeded during normal operation. The containment must be designed to remain leaktight during design-basis-accident conditions.

3.4 SPECIFIC-SYSTEM STRATEGY

In the specific-system strategy, the nuclear plant is required to have specific systems to perform various safety functions. The functions are determined on the basis of conditions expected to occur during an accident. Section IV of Appendix A, 10 CFR 50, provides a good example of this strategy. This section requires that the plant be designed to include (1) a reactor coolant makeup system for protection against small breaks; (2) a residual heat removal system (RHRS) to remove decay heat; (3) an emergency core cooling system (ECCS) to prevent fuel damage following any loss of reactor coolant; (4) a containment heat removal system (CHRS) to remove heat from the containment following a loss-of-coolant accident (LOCA); (5) a containment atmosphere cleanup system (CACS) to control fission products, hydrogen, and oxygen released to the containment atmosphere following a LOCA; and (6) a cooling water system (CWS) to transfer heat from safety systems to the ultimate heat sink during an accident.

3.5 SINGLE-FAILURE STRATEGY

In the single-failure strategy, a system must be designed to perform its intended function, despite the failure of a single component in the system. The actual cause of the failure is not specified. The single-failure strategy is used frequently in the NRC regulations. For example, in describing the RHRS, ECCS, CHRS, CACS, and CWS required by Appendix A, 10 CFR 50, the regulations state that each system must perform its safety function, assuming a single failure. The NRC regulations define single failure to include "multiple failures resulting from a single occurrence." This definition is somewhat broader than the definition of "single-failure strategy" given above, because the NRC definition implies that, in some cases, some actual failure causes would have to be specified if necessary to identify resultant multiple failures.

Another example of the single-failure strategy is General Design Criteria 17, which addresses electric power systems. An onsite electric power system is required that will ensure that vital functions are performed in the event of postulated accidents, assuming a single failure. Note that the postulated accident itself does not constitute the single failure.

3.6 REDUNDANCY STRATEGY

The redundancy strategy, which is related to the single-failure strategy, states that two separate systems or components must be available to perform a particular safety function. In addition, the two systems may be required to be diverse (i.e., based on different operating principles) in order to avoid potential common mode failures. General Design Criterion 17 is based on the redundancy strategy in that two separate electrical power systems (one onsite and one offsite) are required for supplying vital systems. Redundancy is also applied within the offsite system in that two independent circuits are required to connect the offsite transmission network with the onsite electrical distribution system. Another example of the redundancy strategy is General Design Criterion 26, which requires two independent and diverse reactivity control systems.

3.7 FAIL-SAFE STRATEGY

The fail-safe strategy states that a component or system should be designed such that, if a failure occurs, the component or system will fail into a safe state. General Design Criterion 23 provides an example. It requires that the protection system be designed to fail into a safe state if conditions such as loss of electric power, loss of instrument air, or an adverse environment (e.g., extreme heat or cold, fire, pressure, radiation) occur.

3.8 RISK STRATEGY

The risk strategy states that the plant is adequately protected against a particular postulated accident if the frequency with which that accident occurs can be shown to be less than a specified small number, taking into consideration the consequences of such an accident. This strategy is used in NRC Regulatory Guide 1.91, which deals with explosions postulated to occur on transportation routes near the plant. If it can be shown that the probability of such an explosion is less than 10^{-7} per year, then the risk is considered to be acceptably low, and no plant design changes are required to protect against such explosions.

In greater generality, the risk strategy provides for determination that the expected consequences, over all accident sequences, are below some measure. The salient feature of this strategy is that it integrates both consequence and probability of occurrence for each accident sequence.

3.9 DESIGN-BASIS-ACCIDENT STRATEGY

The design-basis-accident strategy requires that the plant be designed such that the consequences of specific, postulated accidents can be shown to be less than specified, acceptable levels. The design-basis accidents determine both (1) the systems that are required to be installed in the plant and (2) the environmental conditions under which these systems must operate. The specified accident may be either mechanistic (i.e., a specific initiating event is defined) or non-mechanistic (i.e., the results of some undefined initiating event are defined). There are many examples of the design-basis-accident strategy in the regulations.

General Design Criterion 2 requires that important safety systems be designed to withstand the effects of natural phenomena, such as earthquakes and tornadoes, during accident conditions. Various regulatory guides provide detailed guidance on how to select the severity of the various natural phenomena. For example, NRC Regulatory Guide 1.59 provides a conservative method for determining the probable maximum flood at any site in the United States.

A LOCA is a design-basis accident frequently mentioned in the regulations. It is defined as loss of reactor coolant from a break in the reactor-coolant boundary, up to and including a break equivalent in size to the double-ended rupture of the largest pipe of the reactor-coolant system. Regulation 10 CFR 50.46 requires an emergency cooling system that will prevent the following limits from being exceeded for a set of LOCAs covering a full range of break sizes and locations:

- Peak cladding temperature of 2200°F;
- Cladding oxidation of 0.17 times the total cladding thickness; and
- Hydrogen generation equal to 1% of the total amount possible from the cladding-water reaction.

Appendix K of 10 CFR 50 describes some of the assumptions to be used in evaluating the performance of an ECCS.

The design-basis-accident strategy is also used in the siting regulations (10 CFR 100). The plant must be sited such that a person standing on the exclusion area boundary for two hours following a postulated fission-product release would not receive an exposure in excess of 25 rems. The quantity of fission products released is to be based on a major accident whose consequences would not be exceeded by any accident considered credible. In practice, the fission-product release is based on a non-mechanistic accident that assumes a release from the core of 100% of the noble gases, 50% of the halogens, and 1% of the solids, and a specified containment leak rate.[20]

4.0 POTENTIAL REGULATORY IMPACTS RESULTING FROM CORE-MELT ACCIDENTS

4.1 SCOPE OF THE TREATMENT

The objective of this study was to consider the impact on Nuclear Regulatory Commission (NRC) regulations, should requirements addressing core-melt accidents (CMAs) be implemented. In fact, this is part of a larger question with which the NRC is faced: should CMAs be treated in the regulations, and if so, how? The approach taken by this report will not answer this question, which is NRC's responsibility in particular. It will, however, provide a perspective and a basis for approaching this rulemaking question based upon results of the study conducted.

Current NRC regulations do not directly address the possibility of the occurrence of a CMA. A goal of existing requirements is to prevent the core from more damage than a small, specified amount as a result of any accident within the current design basis. There are four ways in which implementation of CMA requirements may interact with current regulations. With the discussion in Section 2.0 of prevention vs. mitigation, and the relationship between degraded-core accidents (DCAs) and core-melt accidents (CMAs) as background, these four ways in which requirements would interact with existing regulations may be enumerated as follows:

1. Accidents in which the pressure vessel failure is not the result of a DCA would require specific analysis. Since most of these accidents would appear to be the result of certain common-mode failures (e.g., earthquake, missiles), some decision would be required to determine the extent to which CMA protection would be required as a result of such events, and the degree to which protective systems for CMAs would need to be hardened against these events. For instance, if CMAs were to be treated uniformly in the regulations, it would be reasonable to determine whether CMA protective equipment needs to be seismically qualified. For the most part, such accidents were not considered systematically within this study, since they were judged to be small contributors to risk. However, it should be noted that CMA protection, including CMA mitigation, depends on the accident sequence, as does any other accident protection.

All three remaining interactions will assume the occurrence of a DCA that evolves into a CMA.

2. With the exception of (1) above, the prevention of a DCA implies the prevention of a CMA. The regulatory impact of DCA prevention was documented in the previous study.[2]

3. Likewise, sufficient mitigation of a DCA to prevent reactor vessel failure would prevent a CMA. This was also discussed in the previous study.[2]

4. Any other approach to CMA protection may be considered CMA mitigation. Since current requirements do not address CMA mitigation, new regulations would be required to implement these approaches.

The remainder of this section establishes a basis for considerations involved in implementing new regulations of this type. There would also be probable impacts on existing requirements as by-products of these additions to the regulations. The interaction between new requirements and existing systems and strategies depends heavily on the specific nature of the CMA requirements, and any attempt to document such effects in detail would be highly speculative.

This objective might be based on NRC staff judgment that vented filtered containment mechanisms would increase the safety of nuclear power plants (independent of whether the existing level of safety was adequate or inadequate) and that the cost of implementing these mechanisms was worth the marginal movement in safety. Clearly, extensive modifications to the regulations and associated guidance documents would be required to provide detailed information on the implementation of the vented filtered containment mechanisms, and the overall result would be a prescriptive approach.

An alternative approach or objective might be stated as: "All light-water reactor power plants will provide protection against core-melt accidents." As with the first example, this one might result from NRC staff judgment that such protection would provide a justifiable increase in reactor safety, but would leave the specific approach (e.g., vented filtered containment vs. core-retention devices) up to the licensee.

Both of these examples, if they were real, would be based on the implicit finding that the existing level of safety of nuclear power plants is inadequate, or alternatively, that the risk posed to the public by existing nuclear power plants is too great and that additional measures are required to increase the level of safety (decrease the risk).

In recent years, the NRC has begun to focus more attention on: (1) "What is the existing level of safety as expressed through quantifiable risk measures?"[5] and (2) "What is the appropriate level of safety (risk) for nuclear power plants?"[21] With increased emphasis within the NRC on risk assessment as one of several regulatory tools, potential CMA-related regulatory requirements may be more objectively evaluated in terms of their risk-reduction potential. However, the question remains: "What is the acceptable level of risk due to nuclear power plants?" Once the answer to this question is established, then if it is determined that (1) the risk posed by existing plants is too great and (2) that CMA protection and/or mitigation features offer the potential for risk reduction, the regulatory requirements may be developed based on risk-reduction objectives.

The NRC's recent intiatives toward development of a safety goal[21] indicate that the NRC is moving toward the definition of an appropriate level of safety. Whether this will be accomplished prior to the development of CMA requirements is not known. Nevertheless, we believe that potential regulatory requirements related to CMA protection and/or mitigation should be based on risk considerations either (1) as one of several alternative methods for achieving an acceptable risk level or (2) as a method for reducing existing unacceptable risk levels to acceptable levels.

Even though establishment of a safety goal and of the contribution of CMAs to the overall risk has not yet been determined, it is possible to discuss potential regulatory impacts resulting from consideration of core-melt accidents in light of (1) each of the regulatory strategies described in Section 3.0 and (2) some type of risk-based objective for CMA-related regulatory changes.

4.2 ELEMENTS OF A REGULATORY BASIS FOR CMA PROTECTION

Regulations for CMAs may be constructed from many combinations of preventive/mitigative measures and regulatory strategies. Do any such combinations make more sense than others? What are some important characteristics of various strategies that would be useful for the NRC to consider if it desires to institute regulations for CMA protection? These questions may be partially answered by examining the characteristics of each strategy individually. To a large extent, however, the answers must be evaluated in terms of an underlying rationale for CMA rulemaking. As used here, "rationale" refers to an objective within the scope of NRC authority and to the reasoning that connects the protective measure and associated regulatory strategy with this objective. It is possible for this objective to be phrased in terms of any of the regulatory strategies, and perhaps independently of them as well.

4.2.1 Cost-Benefit Strategy

The use of a cost-benefit strategy would conflict somewhat with the assumption of a risk-based objective. It would imply that the corresponding requirement need not be followed if the ratio of benefit to cost was less favorable than a fixed amount, regardless of the magnitude of the benefit to be achieved (risk reduction, in this case).

However, in practice, some consideration is given to feasibility and to cost effectiveness of proposed requirements. If cost were no obstacle, then small increments in safety would always be possible. Cost and feasibility considerations are more likely to be implicit in the underlying rationale, however, than they are to be of use as an explicit strategy for implementing a given regulatory requirement.

4.2.2 Absolute-Limit Strategy

This strategy could be used in different manners for core-melt rulemaking. One way would be by establishing an absolute limit on one of the risk parameters for CMAs. A requirement could be promulgated, for instance, to limit radiological release due to a CMA to, at most, a specified absolute limit. The underlying rationale associating this requirement with a risk-based objective would be the demonstration that the probability of this occurrence for any plant was less than some quantity that, when combined with the maximum allowed release per occurrence, would yield acceptable risk. The use of this method would clearly require an approved means of demonstrating compliance, which could range from a formal technical evaluation model to the application of NRC judgment. In reality, the latter approach would probably be supplemented through the publication of Regulatory Guides in the form of acceptable systems for limiting release. In this case, the strategy would be functionally equivalent to a specific-system strategy, although some additional flexibility could be provided due to the specification of systems in the Regulatory Guide, as opposed to in the regulations. (See Specific-System Strategy.)

The limits could be applied to new requirements or to existing ones. For instance, some examples of more stringent technical specifications are:

- Increasing the safety limit on the minimum critical power ratio (MCPR). The MCPR indicates how far the fuel cladding is from transition boiling conditions. If the MCPR limit is raised, the safety margin between normal conditions and fuel damage conditions would be increased, which might reduce the chances that a CMA would occur.

- Changing certain trip setpoints in the reactor protection system. These trip setpoints are limiting safety-system settings intended to sense abnormal conditions and then trip the reactor before damage occurs. If certain trip setpoints were changed to more conservative values, the potential for a CMA might be reduced. For example, the reactor vessel water level trip setpoint in a boiling water reactor (BWR) could be raised.

- Making certain limiting conditions for operation more stringent. For example, the standard BWR technical specifications allow power operation with the high-pressure coolant injection (HPCI) inoperable as long as the automatic depressurization system, core-spray system, and low-pressure coolant injection are operable. This could be changed so that power operation would never be possible when the HPCI system is inoperable.

Although the above examples might reduce the probability of a CMA, they should be examined for detrimental effects on day-to-day operation and availability of the plant.

4.2.3 Multiple-Barrier Strategy

The principal use of this strategy would likely be in conjunction with a specific system strategy calling for one of the measures designed to prevent containment failure. For instance, underground siting and double containment represent additional layers of barriers to fission-product release. Compartment venting, bubbling vacuum systems, and some filtered vented containment systems represent partial (not concentric) added barriers, as do schemes for prevention of basemat melt-through (crucible, sacrificial bed, water/steam heat sink). (See Specific-System Strategy and Section 2.0.) Specific effectiveness of each such system would need to be determined, since additional barriers do not necessarily contribute to a risk-reduction objective in the event of a CMA. This is also the reason that specific systems would be required, along with a multiple-barrier strategy, since the effectiveness of this strategy depends on which systems form the barriers.

The existing multiple-barrier approach, as currently used, could also be applied as a basis for requiring that existing barriers be strengthened or augmented to function in the event of a CMA.

This strategy shares many characteristics with the specific-system strategy, since it would likely be used in conjunction with specific systems. It is not, however, as generally applicable.

4.2.4 Specific-System Strategy

Use of this strategy would allow straightforward implementation of requirements and simple testing for compliance. It could be used with any of the specific systems cited or with others to be developed, including existing systems or modifications of them.

One means of implementing such a strategy would be to explicitly and systematically demonstrate the benefit provided by the specified system in terms of risk limitation or reduction. In fact, the explicit connection to the risk objective could be used to derive performance and design requirements for the system, to be included in the specification. Alternately, this strategy could be used in conjunction with others, for instance an absolute-limit strategy, which, in turn, relates directly to satisfaction of the risk objective. As opposed to use of a risk-based strategy directly, all systems to be considered for use must be stated. Although alternatives can be offered by the NRC, each additional system represents additional effort to define and analyze, even if they are never used by a licensee. In effect, the NRC would be adopting part of the effort and initiative of the licensee with regard to design, which is not necessarily to the benefit of the NRC, the public, or the industry. It is unlikely that as flexible a set of alternatives would be presented under this strategy, as compared with a performance-based one such as a risk strategy. On the other hand, standardization of elements of design important for safety, resolution of generic issues, and ease of system design and compliance testing could all benefit in the specific-system approach. It is also unlikely for practical reasons that as much credit could be taken for existing systems and natural process under a specific-system strategy, since that would be a null action. One would expect that a system would be specified for CMA protection only if it differed from existing requirements. It is conceivable, however, that requirements for existing systems could be strengthened in a specification.

Implementation of this strategy without carefully and explicitly relating it to the objective or some derivation of the objective is also a possibility; however this approach contains certain perils. In particular, all parties concerned about CMA rulemaking, industry and intervenors alike, are likely to question the imposition of a requirement or a system whose performance cannot be justified on safety grounds. This could cause delay and extra effort during rulemaking, and perhaps on a case-by-case licensing basis. The support for this conclusion comes from observation of prevalent attitudes, as discussed earlier. It represents a real, pragmatic limitation on the NRC, not a legal or theoretical one.

4.2.5 Single-Failure Strategy

This strategy could be applied to new systems or to existing systems to which it does not already apply (for example, to certain types of containment failure). It could also be modified to a multiple-failure criterion (which would require careful definition and analysis) to reduce the probability of a CMA (i.e., help prevent a CMA).

Existing uses of the single-failure criterion should be re-examined to determine if they are clear and consistent with new requirements for CMA protection. Currently, the design bases for several systems assume a single failure. A possible change to these criteria might be that the given system must tolerate multiple failures to prevent core damage. Another might be that certain additional systems must operate given a single failure.

This strategy is useful only in conjunction with other strategies, in which case it shares some of their characteristics.

4.2.6 Redundancy Strategy

Similar to the single-failure strategy, this could be applied to new systems or to existing ones. A risk-based objective would allow direct analysis of the benefit to be derived from additional redundancy, which is of use primarily where high reliability is required of lower-reliability components/subsystems. Diversity could also be required to reduce potential for common mode failure due to common design, manufacturing, maintenance, etc. It should be noted, however, that the greater the reliability of the system, the less is to be gained from additional redundancy, so that diminishing returns are to be expected.

4.2.7 Fail-Safe Strategy

This could be applied to justify the use of passive safety equipment (e.g., core retention) or to require certain types of operation for systems with possible active components (e.g., certain vented filtered containments).

This strategy, however, has limited use and may be dangerously misleading. Equipment cannot, in general, be "fail safe" under all assumptions and conditions. A pressure relief valve may need to contain pressure at certain times, and to relieve it under other conditions. For such a valve, failing to open may be either a "safe" or "unsafe" failure, depending on circumstances. To some extent, this implies the need for careful analysis of system failure modes and desirable behavior of components, but to some extent it implies the need to be careful in reliance on "fail-safe strategies."

4.2.8 Risk Strategy

This strategy would apply the risk objective's criteria directly to a regulation. For instance, a system could be required to reduce risk from CMA to a given level. Clearly, this strategy would require the least rationale to relate to the underlying objective. It could be used in conjunction with any protective mechanism. It would be "performance oriented" and, hence, allow great flexibility in the choice and design of specific mechanisms. It may allow credit for natural phenomena and existing systems at a level commensurate with understanding at the time. It would place the emphasis for safety evaluation on the NRC, and for design on the licensee.

It is the last point that creates some difficulty with the risk approach. There are some significant uncertainties in current understanding of all the factors influencing risk of power plant operation and its evaluation. These uncertainties exist <u>whether</u> we explicitly assess risk. Many, however, believe that subjective, expert judgment better accounts for the influence of certain unknowns than does explicit risk assessment. Others believe that the very nature of risk modeling provides false confidence in the completeness and accuracy of our knowledge of risk. (This was evident in comments at an NRC meeting on safety goals, held in Harper's Ferry, WV.)[22] These are, to some extent, questions of taste and preference, but must be resolved to determine the proper role and limitations of risk assessment as an explicit regulatory strategy.

Because implementation of this strategy requires risk assessment, it is more difficult to demonstrate compliance of a system as designed or as built than, say, by using a specific-system strategy.

Variations of a risk strategy might address risk of individual elements of the system (function, system, subsystem, component), or might utilize individual factors in the risk equation (probabilities, consequences, or event sequences of various types). Some uses of the absolute-limit strategy reduce to such a variant of risk-assessment strategy. (See that section.) Examples of variants of risk-assessment strategies are:

- The probability of a CMA;
- The probability of some level of reactor core damage (e.g., 50% of cladding oxidized, 10% of noble gas inventory released to primary coolant, MCPR below 1.05 for more than 10 minutes);
- The conditional probability of the offsite dose for the most exposed individual exceeding a specified level, given a CMA;
- The probability of the offsite dose from a CMA exceeding a specified level for the most exposed individual;
- The probability of the offsite dose from all accidents exceeding a specified level for the most exposed individual;
- The societal risks from a CMA, where a societal risk is defined as some function of the CMA frequency and the CMA consequence (e.g., early deaths, delayed cancer deaths, property damage). One possible definition of societal risk is the product of CMA frequency per reactor and total deaths per CMA, so that the units of risk would be deaths per year per reactor. This could be multiplied by reactor lifetime to get units of deaths per reactor. A risk acceptance limit curve, which plots consequences vs. probability, is another way to express a risk limit. Points inside the curve are acceptable, points outside are not; and
- The probability of a particular safety system performing its function.

4.2.9 Design-Basis-Accident Strategy

Design bases exist for the purpose of design of any mechanism. In this strategy, the accident basis would be incorporated explicitly in the regulations.

An obvious strategy for treating CMAs in the regulations is to make a CMA another design-basis accident for which the plant must be designed. [illegible] could be defined mechanistically or non-mechanistically. Possible mechanistic definitions might be: (1) gross failure of the reactor vessel, up to and including a 360° fracture in the circumferential direction; (2) a loss-of-coolant accident (LOCA), as presently defined, followed by complete failure of the emergency core cooling system (ECCS); or (3) a total loss of feedwater, with complete failure of the ECCS. Each of these scenarios could lead to a CMA. A non-mechanistic definition might be: 100% of the reactor core located on the reactor cavity floor, 30 minutes after shutdown.

In addition to defining a CMA, the regulations would have to define successful mitigation of a CMA and provide assumptions to be used in analyzing the performance of CMA mitigating systems. Successful mitigation could be defined in terms of limits that must not be exceeded (like the limits for LOCA mitigation described in 10 CFR 50.46). For example:

- Basemat penetration by the corium shall not exceed 75% of basemat thickness;
- Containment pressure shall not exceed yield strength for slow overpressurization, or ultimate strength for pressure "spikes";
- Two-hour dose at exclusion area boundary shall not exceed 50 rems; and
- Evacuation of population within five miles must occur in less than two hours.

In other words, an absolute-limit strategy might be used with a design-basis strategy.

Another appendix to 10 CFR 50 could be written to describe the assumptions to be used in analyzing the performance of CMA mitigating systems (like Appendix K for LOCAs). Examples of assumptions are:

- The molten corium model shall assume two phases: an oxide layer on top of a metallic layer;

- No fragmentation shall be assumed to occur when the corium initially contacts water in the reactor cavity; and

- Steam explosions shall not be considered.

The use of this strategy would provide explicit requirements necessary for design guidance. The choice of design basis would make explicit the accidents to be managed.

However, it leaves open the possibility that not all accidents of interest will be covered. Depending on the design-basis accidents chosen, and their representation, different characteristics would appear. For instance, certain design-basis accidents specified by conditions existing prior to vessel failure would allow the possible use of preventive measures, while others imply the use of CMA mitigation.

5.0 CONCLUSIONS AND RECOMMENDATIONS

The following are conclusions or recommendations based upon the results of this study:

- Consideration of core-melt-accident (CMA) protection is at a preliminary stage. It would be misleading, at this point, to choose or to recommend a particular mechanism, strategy, or combination of strategies for its introduction.

- The first consideration in CMA rulemaking should be its underlying objective. On the basis of practical considerations, this report has recommended a risk-based objective.

  Based upon this objective, the need for additional CMA protection can, and should, be determined. This desired objective may be demonstrably satisfied by existing systems. If not, it may be satisfied when outstanding questions are resolved regarding phenomenology of CMAs and natural processes.

- If additional protection is required, both the mechanisms and the regulatory strategies chosen determine the effect and form of associated regulations.

- The regulatory strategies may be chosen independently of the risk-based objective; however, each strategy displays certain characteristics that affect its successful implementation. These characteristics, the interactions between a risk-based objective, the individual strategies, and various protective mechanisms are discussed within this report, and would provide a starting point for consideration of factors in the choice of a regulatory approach to CMA protection and the impact of that approach.

- Protective mechanisms may be classified as preventive or mitigative. Prevention of CMAs and their regulatory impact are documented in another report.[2] Mitigation is not, in itself, a new approach, but it is new as applied to CMAs. There are several mechanisms for CMA mitigation that appear to have potential for risk reduction. Mitigation, however, cannot practically cover all situations, since it depends on detailed assumptions of accident initiation and progression just as other accidents do. It would be unreasonable to expect that every possible CMA could be mitigated by practical systems.

- Given that the mitigation of a CMA is not a cure-all, and that the understanding of the risk of a CMA and its phenomena are in a state of flux, balanced consideration should be given to all means by which power reactor risk may achieve acceptable levels, if it does not do so currently.

REFERENCE LIST

1. "Consideration of Degraded or Melted Cores in Safety Regulation." Advance Notice of Proposed Rulemaking. 1980. Federal Register, Vol. 45, No. 193.

2. U.S. NRC. 1981. Effects on NRC Regulatory Guides Resulting from Consideration of Degraded Core (Class 9) Accidents. NUREG/CR-2027. Wash., DC: U.S. NRC.

3. U.S. NRC. 1980. Report of the Zion/Indian Point Study. Vol. 1. NUREG/CR-1410. Wash., DC: U.S. NRC.

4. Darby, J.L. 1981. A Review of the Applicability of Core Retention Concepts to Light Water Reactor Containments. Draft. SAND 81-0416. Albuquerque, NM: Sandia Laboratories.

5. U.S. NRC. 1975. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. WASH-1400. NUREG-75/014. Wash., DC: U.S. NRC.

6. Sherman, M.P. et al. 1980. The Behavior of Hydrogen During Accidents in Light Water Reactors. NUREG/CR-1561. Wash., DC: U.S. NRC.

7. Benjamin, A.S. "Filtered-Vented Containment Systems." Paper presented at International Conference on Current Nuclear Power Plant Safety Issues, Stockholm, October 20-24, 1980. IAEA-CN-39/103.

8. "Interim Requirements Related to Hydrogen Control and Certain Degraded Core Considerations." Proposed Rule. 1980. Federal Register, Vol. 45, No. 193.

9. Petrangeli, G. "Proposed Actions for Safety Improvements After TMI: A Selective Approach." Paper presented at International Conference on Current Nuclear Power Plant Safety Issues, Stockholm, October 20-24, 1980. IAEA-CN-29/52.

10. Berry, D.L. "Decay Heat Removal Systems: Design Criteria and Options." Paper Presented at International Conference on Current Nuclear Power Plant Safety Issues, Stockholm, October 20-24, 1980. IAEA-CN-39/92.

11. McGraw-Hill. 1981. "Safety Goal Should Parallel Degraded Core Rule, Says Interagency Group." Inside NRC. March 23, 1981.

12. Carlson, D.D. and Hickman, J.W. 1978. A Value-Impact Assessment of Alternate Containment Concepts. NUREG/CR-0165. SAND 77-1344. Albuquerque, NM: Sandia National Laboratories.

13. Bukrinski, A.M. "A Bubbling Vacuum System for Limiting the Consequences of a Nuclear Power Plant Accident by a Protective Shell of Under Pressure." Paper presented at International Conference on Current Nuclear Power Plant Safety Issues, Stockholm, October 20-24, 1980. IAEA-CN-39.

14. McGraw-Hill. 1981. "RDA Says Beef up Containments, Avoid PRA and Igniters for Degraded Cores." Inside NRC. January 26, 1981.

15. Walker, D.H. 1980. "AIF Degraded Core Subcommittee - Core Ladle." Paper presented to the AIF Subcommittee on Degraded Cores. Offshore Power Systems.

16. The President's Commission on the Accident at Three Mile Island. 1979. Technical Staff Analysis Report on Alternative Event Sequences. Wash., DC: The President's Commission on the Accident at Three Mile Island.

17. Levenson, M. and Rahn, F. 1980. Realistic Estimates of Consequences of Nuclear Accidents. Palo Alto, CA: Electric Power Research Institute.

18. Aldrich, D.C., McGrath, P.E., and Rassmussen, N.C. 1978. Examination of Offsite Radiological Emergency Measures for Nuclear Reactor Accidents Involving Core Melt. SAND-78-9454. Albuquerque, NM: Sandia National Laboratories.

19. Solomon, K.A. 1980. Some Implications of the Three Mile Island Accident for LMFBR Safety and Licensing: The Design Basis Issue. N-1559-DOE. Santa Monica, CA: Rand Corp.

20. U.S. DOE. 1962. Calculation of Distance Factors for Power and Test Reactor Sites. TID-14844. Wash., DC: U.S. GPO.

21. Office of Policy Evaluation. 1982. Safety Goals for Nuclear Power Plants: A Discussion Paper. NUREG-0880. Wash., DC: U.S. NRC.

22. McGraw-Hill. 1981. "NRC Readies Safety Goal Proposal for Fireworks in Harpers Ferry." Inside NRC. July 13, 1981.

Distribution:

US NRC Distribution Contractor (CDSI) (125)
7300 Pearl Street
Bethesda, MD 20014
100 copies for AN
25 copies for NTIS

M. R. Fleishman (15)
Office of Nuclear Regulatory Research
Division of Risk Analysis
Mail Stop 5650-NL
US Nuclear Regulatory Commission
Washington, DC 20555

J. M. Elliott (8)
International Energy Associates Ltd.
600 New Hampshire Avenue NW
Washington, DC 20037

9400	A. W. Snyder
9410	D. J. McCloskey
9412	J. W. Hickman (20)
9412	N. L. Brisbin
9412	W. R. Cramond
9412	F. T. Harper
9412	A. M. Kolaczkowski
9412	G. J. Kolb
9412	A. C. Payne
9412	R. G. Spulak
9412	T. A. Wheeler
9413	N. R. Ortiz
9414	G. B. Varnado
9416	L. D. Chapman
9420	J. V. Walker
9440	D. A. Dahlgren
9450	J. A. Reuscher
3141	L. J. Erickson (5)
3151	W. L. Garner (3)
8214	M. A. Pound

120555078877 1 AN
US NRC
ADM DIV OF TIDC
POLICY & PUBLICATIONS MGT BR
PDR NUREG COPY
LA 212
WASHINGTON DC 20555