BNL-NUREG-44451
(REV. 7/90)

SAFETY GOALS AND FUNCTIONAL PERFORMANCE CRITERIA*

R. W. Youngblood and W. T. Pratt
Brookhaven National Laboratory
Department of Nuclear Energy
Safety and Risk Evaluation Division
Upton, NY 11973

BNL-NUREG--44451

DE91 004751

and

W. B. Hardin
Advanced Reactors & Generic Issues Branch
Division of Regulatory Applications
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

ABSTRACT

This report discusses a possible approach to the development of functional performance criteria to be applied to evolutionary LWR designs. Key safety functions are first identified; then, criteria are drawn up for each individual function, based on the premise that no single function's projected unreliability should be allowed to exhaust the safety goal frequencies. In the area of core damage prevention, functional criteria are cast in terms of necessary levels of redundancy and diversity of critical equipment. In the area of core damage mitigation (containment), functional performance criteria are cast with the aim of mitigating post-core-melt phenomena with sufficient assurance to eliminate major uncertainties in containment performance.

INTRODUCTION

It is recognized that existing design basis criteria do not by themselves mandate the level of safety performance desired for future plants. The level of safety achieved in the present fleet of operating plants is judged to be adequate, as stated in the Severe Accident Policy Statement,[1] but enhanced safety is desired for future plants. In order to achieve an enhanced level of safety, it is necessary (a) to supplement the single-failure criterion for prevention of core damage, and (b) to supplement design basis loads by requiring containments to handle loads which could occur in severe accidents. It is expected that demonstration of a design's severe accident performance will be accomplished within the framework of a PRA, which is already required by the Severe Accident Policy as formally stipulated in 10 CFR Part 52. The subject of this paper is items a and b. The work discussed here has been performed for the Advanced Reactors & Generic Issues Branch, Division of Regulatory Applications, Office of Nuclear Regulatory Research,

*This work was performed under the auspices of the U.S. Nuclear Regulatory Commission under Contract DE-AC02-76CH00016.

NRC, and will be presented in NUREG/CR-5624 (in preparation).

This paper presents a set of severe accident design criteria which have been developed in order to show what features the design of an evolutionary LWR would need in order to have addressed safety goals proposed for future plants (core damage frequency and large release frequency). Two principles have guided this effort. The first principle is that quantitative safety goals should not be used for numerical comparison with nominal reliability calculations for specific designs; rather, they should be used to develop standards in terms of concrete design attributes. The second principle is based on the observation that since the goals are stated in terms of overall frequency totals, it follows that each safety function should meet the goals individually; decay heat removal failures alone should not exceed the core damage frequency goal, and so on. Rather than specifying percentiles of uncertainty distributions, the formulation adopted here is that the design of each safety function should be sufficiently robust that its failures alone do not *nominally* contribute to core damage frequency or large release frequency at levels which are comparable to the goals. This formulation leads to functional performance criteria, but does not constitute an allocation of performance over safety furctions; rather, it constitutes a set of high-level boundary conditions which allocation procedures should arguably obey. Based on order-of-magnitude reliability arguments and phenomenological analyses, the criteria are stated in terms of recommended levels of redundancy, diversity, and physical capacity. The recommendations have been made in light of the need to preclude by design certain major phenomenological uncertainties in severe accident performance.

The present work was originally carried out in order to support implementation of a core damage frequency goal of 10^{-5} per year, as recommended in the SECY-89-102[2] (March 30, 1989) Commission paper on implementation of safety goals. More recently,[3] the Commission has issued guidance which contemplates a core damage frequency goal of 10^{-4} per year, a large release frequency goal of 10^{-6} per year, and a conditional containment failure probability goal of 0.1. This initially suggests that the present recommendations aimed at core damage prevention may have been carried too far; however, such a conclusion is premature. A comparable development has yet to be carried out even for implementation of a core damage frequency goal of 10^{-4} per year; present review criteria are not explicitly based on safety goal arguments at any level. Moreover, unless an unprecedentedly robust containment design is presented, much of the present development is applicable simply on the basis of the

large release goal of 10^{-6} per year; some designs which meet a 10^{-6} large release goal and a 0.1 containment failure probability goal will need to strive for attainment of a 10^{-5} core damage frequency goal. In short, while this report documents recommendations which may need updating in light of recent policy developments, all of the recommendations on containment performance continue to apply, and many of the present recommendations on core damage prevention may, on closer examination, continue to be supportable even if the nominal core damage prevention goal is placed at 10^{-4} per year rather than 10^{-5} per year.

The scope of this paper is limited to accidents initiated by "internal events" occurring during power operation, and the focus of the paper is on the redundancy, diversity, and capacity of key design features in evolutionary LWRs. In order to meet the safety goals, it is necessary to address accidents initiated by external events. It is not believed that the present recommendations would be altered by these additional considerations; rather, supplementary guidance is needed to address the effects of such events on the key systems, and will be developed separately. Similarly, it is necessary to address accidents initiated during modes of operation other than full power. While it does not appear likely that such considerations would warrant further increases in system redundancy, LCOs for nonpower modes need to be reconsidered, and this could affect system design. This issue should be explored further.

SEVERE ACCIDENT CRITERIA FOR CORE DAMAGE PREVENTION

The proposed safety goal frequencies are very ambitious. In order to meet them, extra (beyond-single-failure) defense in depth will be necessary. This comment implies a certain relationship between redundancy and absolute reliability; formally, one could imagine meeting an ambitious goal with a small number of trains having extremely low failure probability, but this approach is academic. In PRAs of commercial nuclear power plants, a standby fluid system consisting of two trains is generally assessed to have a failure-on-demand probability on the order of 10^{-4} to 10^{-3}. A more redundant system may have a somewhat lower probability of failure, but common cause failure modes tend to limit the gains in reliability which might otherwise be imagined to ensue from the addition of trains. In particular, it is very difficult to credit a system-level failure-on-demand probability on the order of 10^{-6} or less at least for an active system (as opposed to a completely passive safety feature). Therefore, if a *function*-level failure-on-demand probability of order 10^{-6} or less is needed (e.g., to meet the proposed 10^{-5} per year GDF goal), it is necessary to be able to perform this function by

either of two distinct systems, each being sufficiently redundant and diverse to have a fairly low failure-on-demand probability. This formulation is simply a particular instance of a defense-in-depth philosophy: it is the form that a defense-in-depth criterion takes in the context of a semiquantitative reliability scale.

Depending on the claims made for containment performance, this high level of functional reliability might be needed in order to support the large release goal, even if the core damage frequency goal is set at 10^{-4} per year rather than 10^{-5} per year. For brevity, the discussion in the following sections refers to the "proposed" safety goal, by which is meant a core damage frequency of 10^{-5} per year.

Here, 'distinct' means that the attributes of the two systems should differ enough that their failures are not causally linked to a degree sufficient to compromise the intended functional reliability. Much work has gone into assessment of common cause likelihoods, how far to go in postulating coupling between hardware, across system boundaries, etc. From this work, it is clear that diversity is necessary in order to meet the safety goals using active systems; however, it is not clear that a general standard of "diversity" imposed at the conceptual design stage can guarantee the desired level of system performance. Therefore, in the present context of PRA based on design of future reactors, this topic becomes an interface issue, part of "making the PRA come true." When the PRA takes credit for independence of layers of defense in depth, and for robustness against common causes of failure, steps must be taken during construction and operation to assure that this independence is real.

Reactor Shutdown

In order not to exhaust the proposed safety goal on CDF, the contribution of ATWS sequences to core damage frequency must be kept substantially below 10^{-5} per year. This means that the product {challenge rate}*{probability of core damage, given a challenge} must be significantly less than 10^{-5}. In existing plants, the rate at which reactivity control is challenged is on the order of several events per year (from normal transients). It is hoped that future plants will reduce this rate to about one per year; for purposes of illustration, let us assume that this challenge rate (1/yr) is the basis for a requirement on reactivity control. Then the probability of ATWS core damage given a normal transient should be significantly less than 10^{-5} (i.e., it should be of order 10^{-6}).

It was argued above that alleged system failure probabilities as low as 10^{-6} per demand are not credible. Therefore, given the challenge rate, it would be unacceptable

to rely *entirely* on a single *active* system to prevent ATWS core damage. Therefore, it is necessary to take credit for measures to be adopted after RPS failure. Existing PRAs do not stop with failure of the RPS; given failure of the RPS, core damage becomes a possibility in some scenarios, but given suitable pressure relief and application of other control measures, and perhaps barring unfavorable moderator conditions, the plant is able to handle the transient while things are brought under control.

Existing PRA work suggests mean ATWS CDFs ranging downwards from a high in excess of 10^{-5} per year. For Westinghouse PWRs, the CDFs are relatively low on this scale, for reasons having to do with design attributes not necessarily shared by other plant types. CDFs reported for other PWR plant types, while not "high," are not low in the context of the present aspirational safety goal. Finally, for existing BWRs, the arguments driving the CDF downward rely very heavily on presumed operator actions.

Thus, existing hardware requirements (DBA analysis plus ATWS rule[4]) do not by themselves drive ATWS CDF down sufficiently to justify arguing that those requirements adequately serve the proposed 10^{-5} CDF goal. For BWRs, in order to convincingly claim a low CDF for ATWS, one must invoke significant involvement of the operational staff in handling the scenario. For purposes of reviewing advanced designs, it seems inappropriate to consider fulfilling high-level performance objectives by relying extensively on operator behavior in complex scenarios. At the same time, it is believed that advanced designs can reasonably be expected to approach safety goal performance without recourse to extensive credit for operator action in ATWS scenarios. If this point is accepted, then for BWRs, one must supplement the hitherto-required hardware with more hardware and/or physical margin. For PWRs, it is appropriate at least to lock in and enhance the design features of those plants whose ATWS frequency is low, and to reduce even further the remaining dependence on operator action.

The form of the functional performance criterion in this area is therefore as follows. The plant should have two "systems" [layers of defense] which collectively bring the functional failure probability down to the 10^{-6} range:

(1) the RPS, and

(2) either

(a) a diverse, automatic, fast-acting alternative shutdown system coupled with the ability to tolerate ATWS conditions while the scenario is brought under control, or

(b) a possibly more relaxed shutdown capability, combined with a demonstration that RPS

failure is significantly more benign in the new design than it is for existing LWRs.

This is not a radical departure from existing practice (unless automation qualifies as a radical departure), but there are two key practical differences. First, the thrust of the criterion is to reduce very significantly the role of the operator in management of the early stages of the scenario. Secondly, the RPS is presently reviewed much more formally than the other features (the beyond-design-basis attributes invoked to get ATWS frequency down); but casting the criterion in this way means that in future plants, the second line of defense would also be scrutinized very carefully (e.g., plant response to ATWS, behavior and reliability of liquid poison systems, pressure relief, etc.). This could lead to technical specifications on equipment for which they are presently deemed unnecessary.

Primary Coolant Inventory

Consider first the function of inventory makeup following a loss of coolant. For purposes of illustration, the challenge frequency of this function is taken here to be on the order of 10^{-2} per year. (This is a characteristic small LOCA frequency used in PRAs; it may be conservative for future plants, because its applicability to existing plants is based in part on seal LOCAs and pressurizer valve LOCAs, which may be largely engineered out of future plants.) By arguments similar to those given above, then, the coolant makeup function for small breaks should be a 10^{-4} system: given a challenge, the probability of functional failure should not be significantly greater than 10^{-4}, if we are to achieve an overall CDF contribution level on the order of 10^{-6} or less. It is doubtful whether a system which is merely single-failure-proof could be considered adequate by this criterion. This objective might be approachable by a single system having a high degree of redundancy; it can be met more easily (and more convincingly) if a diverse means of makeup is available, as it is in plants which can reliably depressurize to a pressure where lower-head injection systems may be brought into play.

For existing plants, the sequence consisting of "interfacing system LOCA bypassing containment and leading to core damage" is generally assessed to have a frequency which is relatively low (on the order of 10^{-6} per year or less), even in the context of the present core damage frequency goal for advanced LWRs; but interfacing LOCA frequency is not negligible in the context of the proposed goal for the frequency of large releases, which is 10^{-6} per year. For purposes of meeting this large-release goal, it is desirable either to render interfacing LOCA essentially incredible (e.g., by reducing its frequency to that of

multiple independent passive failures), to design the plant so that containment bypass does not result if low pressure systems are overpressurized and failed, and to design so that the mitigating function is not adversely affected by the initiating event (that is, some injection capability should survive the overpressurization). Failure of multiple check valves constitutes a multiple passive failure, but does not necessarily constitute multiple *independent* passive failures.

The proposed criteria are as follows:

the design against interfacing LOCA should incorporate multiple independent passive barriers against containment bypass;

interfacing LOCA should not fail the inventory makeup function;

major interfacing systems should be able to withstand RCS conditions (ultimate capacity, not design basis);

the function of LOCA mitigation should be double-active-failure-proof, including switchover to recirculation phase (if any), using best-estimate capacity requirement;

no single active component failure (including bus faults) should initiate a LOCA;

no loss of a single support system (service water, component cooling water, electric power) necessary to inventory makeup should initiate a LOCA. This is intended to apply to such things as pump seal cooling and primary relief valve operation.

The criteria for LOCA mitigation are less stringent than those derived for reactivity control and decay heat removal, because inventory makeup is challenged much less frequently than reactivity control or decay heat removal. The proscription against containment bypass is necessary because the large-release goal is very ambitious. Criteria aimed at LOCA prevention are included because it is necessary to ensure a relatively low LOCA frequency, in order to justify *not* requiring diversity in the inventory makeup function, by analogy with the requirement on decay heat removal.

Decay Heat Removal

As for reactivity control, the safety function of removing decay heat is challenged on the order of once per year (more, for most existing plants). By arguments given above, this means that the functional failure-on-demand probability should be driven down to the order of 10^{-6}, and again, it is inappropriate to rely on a single active system when the functional reliability is required to be so high.

The capacity required of systems performing the function of early decay heat removal is determined by the

objectives of (a) assuring adequate core cooling immediately following reactor trip, and (b) ultimately reaching cold shutdown. Given that we are confining ourselves to active safety features, the reliability criterion for early decay heat removal is as follows.

The function should be capable of fulfillment by either of two distinct and diverse systems, each highly reliable, the reliability to be achieved through redundancy. Each should be at least single-active-failure-proof, and the overall complement of equipment should be sufficiently diverse to eliminate concerns of common-cause failure of the entire function.

The function as a whole should be able to withstand two active failures, given a loss of offsite power. This is to be understood as extending down through support systems.

CONTAINMENT

The Commission paper on safety goal implementation[1] originally recommended a core damage frequency goal of 10^{-5} events/year and a large release frequency goal of 10^{-6} events/year. This formulation implicitly contemplated a particular balance between prevention and mitigation, without explicitly defining a figure of merit for the mitigation function. More recently, the Commission has endorsed a conditional containment failure probability (CCFP) goal of 0.1. Thus, the considered intention regarding containment design is (and has been) a containment design which has approximately a 90% chance of succeeding, given a severe accident challenge. Even though the implied failure probability is numerically greater than that commonly associated with engineered safety features involved with core damage prevention, such a containment constitutes an important layer of defense, and the demonstration of the physical capacities required in severe accidents is nontrivial.

In addition to the CCFP goal discussed above, the Commission has considered a deterministic criterion intended to assure that fission products will decay to below 10 CFR 100 limits before a significant release occurs. The thrust of this criterion is to assure adequate long-term removal of decay heat from containment. This is complementary to the thrust of the CCFP goal, which is intended to address early challenges to containment integrity.

Phenomenological Considerations

Containments for evolutionary LWRs must have a relatively high likelihood of containing the loads expected from core meltdown accidents. This calls for design criteria which go beyond existing requirements in some areas, because existing containments are designed to contain the pressure and temperature loads resulting from ***design basis*** loss-of-coolant accidents (LOCAs), and these loads are

not necessarily characteristic of severe accidents. On the other hand, severe accident loads are not to become the new design basis loads; rather, the goal is to formulate criteria whose effect is to include severe accident loads within the *ultimate capability* of containment. For example, a containment designed for an internal pressure of 50 psig might well contain a pressure pulse of 90 psi resulting from a H_2 combustion event, even though this pressure is beyond its design limit.

The safety margins in existing plants have been the subject of considerable research and evaluation, and these studies have indicated the ability of containment systems to survive pressure challenges of 2.5 to 3 times the design levels. Some existing containment designs use a large internal volume and high design pressure to accommodate the rapid pressure and temperature loads associated with LOCAs. Other containment designs use pressure suppression devices (pools of water or ice chests) to condense the steam. Containments that utilize pressure suppression devices usually have smaller volumes and lower design pressures than containments that do not use these devices. In addition, most containments (with or without pressure suppression) use spray systems for long term heat removal and atmospheric decontamination. Additional requirements were placed on some containment designs after the accident at TMI-2. The interim H_2 rule[5] requires BWRs with Mark I and II containments to operate with an inert atmosphere. In addition, BWRs with Mark III and PWRs with ice condenser containments are now required to operate with a deliberate ignition system installed. Large volume and subatmospheric containments were not given any additional requirements as a result of this rule.

In summary, then, the various containment types presently utilized in U.S. nuclear power plants have the capability to cope, to varying degrees, with many of the challenges presented by severe accidents. However, there are challenges to containment integrity which could occur prior to or during a core melt accident, which might lead to possible release of fission products outside of containment. The approach taken here for the evolutionary LWRs is to develop functional performance criteria which address those challenges that have been found to have the largest contribution to uncertainty in containment performance. This approach provides reasonable assurance of the ability of containment to withstand severe accident loads, without attempting to achieve an extremely low frequency of large release by containment design alone.

In light of the above, the present approach is to provide best-estimate recommendations for ultimate capacities which accommodate severe accident challenges, based on insights gained from analysis of significant

challenges to containments at existing plants, and on the results of severe accident research. These recommendations supplement IE-type requirements of redundancy and design capacity for design basis events, and address the containment performance objectives (both the CCFP goal and the qualitative goal articulated in the Introduction to this paper).

Major Challenges to Containment

The approach taken here is to develop performance criteria for those challenges that were identified in NUREG-1150[6,7] and in previous studies as being important contributors to uncertainty in containment performance for each of the plants considered. Five severe accident containment challenges have been identified as major contributors to uncertainty in containment performance. The five challenges are hydrogen combustion, high pressure meltdown phenomena, containment bypass, core debris/containment interactions, and long-term decay heat removal. Performance criteria for the above challenges are developed in the following sections. These criteria aimed at achieving a level of containment performance which contributes significantly to risk reduction (e.g., a 90% likelihood of containment success) without necessitating overdesign.

Reducing uncertainty in containment performance is an important element of the present approach. "Best estimate" performance cannot be said to satisfy safety goals if it is subject to significant uncertainty. Based on the extensive studies and data that currently exist for evolutionary containment designs, it is believed that compliance with the particular set of functional containment performance goals identified in this paper would resolve uncertainty to the extent necessary to achieve the

proposed safety goals. Accordingly, extended further debate on these technical issues should not be necessary. In addition, the need for detailed analyses of the associated complex severe accident phenomena should be greatly reduced, although it may still be necessary to do some analyses to evaluate specific design solutions. Alternative approaches may also be adequate if submitted with appropriate justification.

Severe Accident Criteria for Containment Performance

Hydrogen

Estimating the amount of hydrogen that might be generated during a full core meltdown accident is subject to considerable uncertainty. The EPRI Advanced light water Reactor Document[8] concludes that "hydrogen, in excess of the equivalent resulting from oxidation of 75% of the active fuel clad, need not be considered." However, 10 CFR 50.34(f) addresses full core meltdown accidents and specifies that hydrogen equivalent to oxidation of 100% of the active cladding be considered.

Thus, it is suggested that hydrogen generation equivalent to 100% clad oxidation be considered for full core meltdown accidents in evolutionary LWRs. However, it should be noted that this recommendation is conditional on a relatively rapid cooldown and formation of a coolable debris bed in the reactor cavity. Ways to assure a coolable debris bed are discussed below under "Core Debris / Containment Interactions."

The next issue to be addressed is how to demonstrate that the various evolutionary containment designs can accommodate 100% clad oxidation. If one assumes the deflagration of all of the hydrogen, one can straightforwardly estimate a maximum pressure rise and determine whether or not this is within the ultimate capacity of the containment. However, it is possible under some circumstances to produce a detonation wave; such a wave could impose dynamic loads on the containment boundary which would greatly exceed the equivalent static loads from hydrogen deflagration. In fact, detonation loads have been calculated to be sufficiently damaging to cause failure of some LWR containments. It is much more difficult to predict the dynamic loads associated with detonations than to predict the equivalent static loads associated with deflagrations. Given the uncertainties associated with calculating detonation waves, and the uncertainty of the response of containments to these dynamic loads, it is prudent to minimize the possibility of detonations in the containments of evolutionary LWRs.

Detonations are usually predicted to occur at relatively high hydrogen concentrations, although there is experimental evidence to suggest that hydrogen combustion can experience a

deflagration - to - detonation (DTD) transition at relatively low hydrogen concentrations. The EPRI ALWR Requirements Document suggests that if hydrogen concentrations are maintained below 13% by volume, then a detonation is unlikely to occur. This value is also based on the technical arguments in the FAI document[9]. However, there are experimental data which indicate that detonations are possible at concentrations on the order of 10%. 10 CFR 50.34(f) requires that hydrogen generation equivalent to oxidation of 100% of the cladding be considered (which is consistent with the above conclusion) and that the volumetric concentration of this quantity of hydrogen be below 10% of the containment free volume.

The hydrogen control measures needed to comply with 10 CFR 50.34(f) would eliminate hydrogen combustion as a potential threat to containment integrity in the evolutionary LWRs, *for core meltdown accidents in which the primary system is at low pressure*. Thus the functional performance criterion for hydrogen control is to comply with 10 CFR 50.34(f). However, these measures cannot mitigate the effects of a core meltdown accident in which the primary system remains at high pressure. Mitigation of high pressure meltdown accidents is addressed in the following section.

High Pressure Meltdown Events

If the primary system of an LWR remains at high pressure during a core meltdown accident the integrity of containment can be challenged in two ways.

Firstly, natural circulation between the hot reactor core and the rest of the primary system can cause significant redistribution of heat. This can cause high temperatures in parts of the primary system remote from the core. It has been suggested that high temperatures and pressures in the primary system might cause failure of the reactor coolant pump seals or the steam generator (SG) tubes. Induced failure of the SG tubes is of concern, because if relief valves in the secondary system are open then a direct path would be open from the damaged reactor core to the environment (i.e., containment would be bypassed). In the first draft of NUREG-1150,[6] the probability of induced SG tube rupture was given at 0.15, conditional on a high pressure core meltdown event.

The second challenge to containment integrity occurs after the core debris relocates into the bottom of the reactor vessel and melts through it. If the primary system is at high pressure, the core debris will be ejected from the vessel under pressure. It has been postulated that under these circumstances, the ejected core debris would be dispersed into the containment atmosphere as fine particles and directly heat it. In addition, the metallic components of the ejected core debris can react with oxygen

and steam producing chemical energy, which further heats the containment atmosphere. This process has been termed direct containment heating (DCH). In addition, DCH can further load the containment atmosphere by causing the recombination of hydrogen with free oxygen even though the hydrogen concentration is below conventional flammable limits. If there is water in the reactor cavity at the time of dispersal, the pressurized stream of molten core materials could cause steam explosions which could further fragment and disperse the debris. Effects of the high temperatures caused by DCH on containment structure and equipment are also cause for concern. The issue of DCH is highly controversial because it has the potential to significantly change the risk profile of a plant. Under pessimistic assumptions, DCH provides a mechanism to fail a containment relatively early, whereas more optimistic assumptions predict a lower probability of early failure. However, there is still a significant potential for early containment failure for some containment designs.[6,7] The potential for early failure is caused by a combination of primary system depressurization, hydrogen combustion, and rapid steam generation at the time of reactor vessel meltthrough. Thus, even if DCH does not occur, other phenomena associated with high pressure core meltdown accidents still have the potential to cause early failure in some containment designs.

Evolutionary LWRs should address the above concerns related to high pressure core meltdown accidents. One acceptable way of addressing both of these concerns is to provide a reliable means of depressurizing the primary system. Depressurization eliminates the concerns related to induced SG tube rupture and lowers the pressure and temperature loads at vessel failure to such a level that they no longer have the potential to cause early failure.

Careful analysis will be necessary in order to determine how best to achieve the goals of depressurization while avoiding adverse effects (e.g., enhanced H_2 generation due to depressurizing at the wrong time).

Containment Bypass

Two ways in which an early loss of containment integrity can result are an isolation failure and a containment bypass.

Isolation failure results from a failure to establish containment integrity prior to or following the onset of an accident. It refers to excessive leakage rather than the total loss of containment integrity. For example, failure to close personnel air locks or a large vent valve would constitute an isolation failure. A pre-existing leak rate in excess of allowable leakage from the containment can also constitute an isolation failure. In past studies isolation failures

have been found to be relative low frequency events.

Containment bypass refers to several different situations. One kind of bypass is caused by an interfacing system loss-of-coolant accident (LOCA) where there is a failure in the barriers between the high pressure reactor coolant system and an interfacing system, part of which is outside of primary containment. Such events can occur in both PWRs and BWRs due to failure or inadvertent opening of valves or equipment which are part of the interface between the primary and secondary systems. These events were dealt with under "Inventory Control." In PWRs, steam generator tube rupture represents a special case of interfacing systems LOCA. Another type of bypass can occur when an important functional part of the containment is bypassed. Suppression pool bypass in BWRs and bypass of the ice bed in ice condenser PWR containments constitute this kind of problem.

Core Debris/Containment Boundary Interactions

During a severe accident, after the core debris melts through the reactor vessel, it will begin to interact with structures in the region below the reactor vessel. After the core debris leaves the vessel it can pose a short term or a long term threat to containment integrity.

A short term threat to containment integrity occurs if the core debris can contact the containment boundary and melt through it very rapidly. Some existing BWRs with Mark I containments were found[6,7] to be susceptible to this failure mode. The impact of this failure mode (called liner meltthrough) on early containment failure at Peach Bottom (which is a BWR with a Mark I containment) was found in both drafts of NUREG-1150[6,7] to be significant. Given the impact that this failure can have on containment performance, it is important to preclude it in evolutionary LWRs by appropriate configuration of the containment.

A long term threat to containment integrity may occur if the core debris is confined into a deep configuration, which would tend to keep it hot and promote extensive interactions with the concrete basemat. Such a configuration will produce extensive fission product release and large quantities of hot noncondensible gases, which would heat, pressurize, and eventually fail the containment. In addition, this configuration would be more likely to cause the core debris to penetrate the concrete basemat and in some designs could fail containment by meltthrough. Phenomena associated with core debris interacting with concrete in the ex-vessel configuration are highly uncertain; however, some general guidelines are appropriate for evolutionary LWRs. For example, it is clear that spreading the core debris over a large surface

area will rapidly cool it and minimize fission product release, gas generation and core/concrete interactions. Also, water addition to the core debris can be beneficial. Although water on top of the core debris may not be capable of penetrating the debris and cooling it (because of crusts), water does trap fission products generated by core/concrete interactions and it is an additional heat sink. In addition, it is possible to construct the reactor cavity regions with a structural material that would not result in extensive gas release when attacked by the core debris.

The functional performance criteria in this area are as follows:

1. There should be no direct pathway for core debris to contact and cause failure of the containment wall.

2. There should be sufficient floor area to enhance debris spreading and reduce the potential for other structural degradation that could lead to containment failure.

3. There should be provision for flooding the core debris.

4. Materials should be selected to reduce generation of gases as a result interactions with the core debis.

Long-Term Decay Heat Removal

During a severe accident, the containment heat removal systems could fail. If these systems are not restored, the pressure in containment will continue to rise and could exceed the ultimate pressure capability. In both drafts of NUREG-1150,[6,7] all of the reactors analyzed were found to be susceptible to late containment failure caused by loss of containment heat removal. This can lead to a relatively significant release, but the release occurs after a relatively long waiting period; thus, the consequences associated with this scenario are confined to latent health effects, land contamination, on-site costs, etc. This scenario can be prevented in some designs by controlled venting; however, no loss of containment integrity (including venting) can be permitted to occur before a minimum time period after scram.

Maintaining containment integrity for a minimum period (e.g., 24 hours) is based on providing sufficient time for the remaining airborne activity in the containment (principally noble gases and iodine) to decay to a level that would not exceed 10 CFR Part 100 dose guideline values when analyzed realistically, if controlled venting were to occur after that time.

The following general criterion for long-term containment performance is appropriate:

> The containment should maintain its role as a reliable leak-tight barrier for a minimum period of 24 hours following the onset of core damage, and ensure that following this 24-hour period, the containment will continue to provide a barrier against the uncontrolled release of fission products.

During this period, containment integrity should be provided, to the extent practicable, by the passive capability of the containment itself and any related passive design features (e.g., suppression pool). Following this period, the containment should continue to provide a barrier against the uncontrolled release of fission products. However, in keeping with the concept of allowing for intervention in coping with long-term or gradual energy release, after this minimum period, the containment design may utilize controlled, elevated venting to reduce the probability of a catastrophic failure of the containment. Alternatively, a design may utilize diverse containment heat removal systems or rely on the restoration of normal containment heat removal capability if sufficient time is available for major recovery actions (e.g., 48 hours).

SUMMARY

This paper has presented a set of design attributes which are considered to be necessary in order for evolutionary LWR designs to fulfill safety goals which were proposed for future plants. The proposed safety goal for core damage prevention (10^{-5} events per year) warrants levels of redundancy and diversity in the decay heat removal function which go beyond requirements for existing plants. Similar arguments lead to enhanced capabilities for coping with ATWS, and increased attention to preventing LOCA initiating events. The proposed goal for conditional containment failure probability warrants enhanced containment capabilities in several areas, in order to substantially reduce the uncertainty surrounding the severe accident performance of containments built to today's design basis requirements. These enhanced capabilities include hydrogen mitigation, avoidance of high-pressure melt scenarios (or significantly improved capability for surviving them), prevent adverse effects of core debris/containment interactions (design to achieve desired depth, minimize gas generation, allow for flooding of debris), and long-term removal of decay heat in full-scale core melt scenarios.

REFERENCES

1. NRC Policy on Future Reactor Designs, NUREG-1070 (U. S. Nuclear Regulatory Commission, July 1985).

2. Implementation of Safety Goal Policy, SECY-89-102 (U.S.

Nuclear Regulatory Commission, March 30, 1989).

3. Staff Requirements Memorandum on "SECY-89-102-Implementation of the Safety Goals", U. S. Nuclear Regulatory Commission, June 18, 1990.

4. ATWS Final Rule - Code of Federal Regulations, Title 10, Section 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram Events for Light-Water Cooled Nuclear Power Plants," (June 1984).

5. Federal Register, Volume 50, No. 17, Friday, January 25, 1985, 10 CFR Part 50, "Hydrogen Control Requirements."

6. Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150 (Draft for Comment, U.S. Nuclear Regulatory Commission, February 1987). See also supporting documentation.

7. Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150 (Second Draft for Peer Review, U.S. Nuclear Regulatory Commission, June 1989). See also supporting documentation.

8. Advanced Light Water Reactor Requirements Document (EPRI [Electric Power Research Instititue], Palo Alto, California).

9. Technical Support for the Hydrogen Control Requirement for the EPRI Advanced Water Reactor Requirements Document, October 1989, Fauske & Associates, Inc.

- END -

DATE FILMED

12 / 28 / 90