

Shapar

DOCKET NUMBER DR 50
PROPOSED RULE DR 50

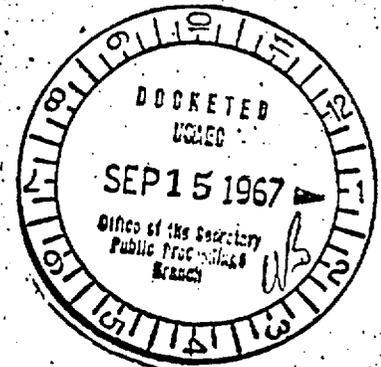
OAK RIDGE NATIONAL LABORATORY

OPERATED BY
UNION CARBIDE CORPORATION
NUCLEAR DIVISION



POST OFFICE BOX Y
OAK RIDGE, TENNESSEE 37830

September 6, 1967



Mr. H. L. Price
Director of Regulation
U.S. Atomic Energy Commission
Washington, D. C. 20545

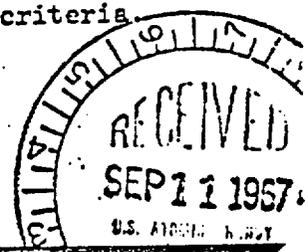
Dear Mr. Price:

Subject: Review of USAEC "General Design Criteria for Nuclear Power Plant Construction Permits" Federal Register, July 11, 1967

The subject document has been reviewed by members of the staff of the Nuclear Safety Information Center. We realize and appreciate the great amount of work that your staff has done in bringing these criteria to their present form. We participated in the initial review of the criteria when they were issued in November 1965 and we are pleased to have the opportunity to review this later version. Our comments are enclosed in two parts: (1) general comments which apply to the entire set of criteria and (2) specific comments on the individual criteria and in a few cases on sections such as VII, Engineered Safety Features.

With a few exceptions, the scope of the criteria seems broad enough and generally well organized. We do have rather extensive comments on those criteria which deal with protection systems. A difficult problem is that of assessing reliability. The "single failure criterion" is an attempt to relieve this situation, but its application is subjective and it has different meanings to different individuals. Another problem area is that of the use of the same instruments for both operating the plant and providing protection. We believe that such interdependence can only degrade the reliability and performance of the protection system. Problems such as these make the task of writing criteria and standards quite difficult.

Further, the absence of clear definitions of terms, which to many are rather loosely understood, could limit the effectiveness of the criteria. We feel that there is a critical need for these definitions.



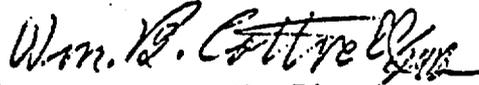
Mr. H. L. Price

-2-

September 6, 1967

We again wish to commend you for the significant contribution represented by these criteria. If you have questions concerning our comments, we will be glad to discuss them with you.

Sincerely yours,



Wm. B. Cottrell, Director
Nuclear Safety Information Center

WBC:JRB:jt

Enclosure

cc A. J. Pressesky

General Comments

1. The ramifications of civil disobedience, riots, strikes, sabotage, and the like have not even been mentioned. With this vast potential risk in mind, should not the physical security of the plant be considered?
2. Since these criteria will be used by many groups whose terminology is not always (or even usually) in agreement, a set of definitions is badly needed. For example - what is a system, component, engineered safety feature, failure, redundancy, channel, surveillance, monitoring, malfunction, protection system, loss of coolant accident, etc.?
3. Since "single failure criteria" are to be applied to systems other than those for control (for which criterion 21 is the definition), it is extremely important that they be clearly defined for all systems.
4. Since the introduction uses the phrase "nuclear reactor plant" why is the phrase "reactor facility" used in the text of several of the criteria to mean the same thing?

Specific Comments

Title - General Design Criteria for Nuclear Power Plant Construction Permits

The title is really not grammatically correct, since it infers that we are designing a "construction permit".

Criterion 2 - Performance Standards

1. Line 7: Delete "performance" since this could be construed as applying to operating performance only.
2. In regard to earthquakes the "appropriate margin for withstanding forces greater than those recorded . . ." has not been defined here and furthermore it would be extremely difficult to do so at least with our present understanding of earthquake phenomena. Therefore, the criterion should state what constitutes an adequate margin.

Criterion 4 - Sharing of Systems

We agree with criterion 4 as it applies to the nuclear reactor plant but it should be extended to apply to systems, sub-systems, and especially engineered safety features.

Criterion 5 - Records Requirements

1. Line 2: Should read, "Records of the design, fabrication, inspection, testing and construction of . . ." to be sufficiently inclusive. The performance of engineered safety features must be determined as a datum for evaluation of subsequent tests required of the system. For example, criterion 46 states that active components be periodically tested for required performance.
2. Line 5: Change "its" to "his" to refer to the operator's control.

Criterion 8 - Overall Power Coefficient

For this entire criterion it might be better to say that "the reactor shall be designed so that either the overall power coefficient in the power operating range shall not be positive or reliable controls which will eliminate or minimize the undesirable effects of a positive power coefficient shall be provided, tested and proved effective."

Criterion 10 - Containment

We infer from subsequent criteria that the protection system is not considered an engineered safety feature even though there are reactors that depend upon the protection systems to work in order not to overstress the containment. Thus, either "engineered safety features" should be defined to include the reactor protective system, i.e., scram functions, or this and other functions should be specifically mentioned. We prefer the former alternative.

Criterion 11 - Control Room

The aims of this criterion are certainly desirable but it is difficult if not impossible to prove the criterion has been met. However, some clarification is needed, for example, if a fire in a panel renders the controls of some emergency system inoperable, the criterion can be interpreted to mean that two separate control rooms are required. Is this the intent?

Criterion 13 - Fission Process Monitors and Controls

1. Line 4: Delete "throughout core life and" since it is redundant.
2. The examples cited should either be deleted or augmented by a more comprehensive set including flux, hot spots, etc.

Criteria 14 and 15 - Core Protection Systems and Engineered Safety Features

These criteria exemplify the fact that a more detailed definition of containment and engineered safety features needs to be included. One could define the engineered safety features as including scram system, core protection system, etc., and then eliminate Criterion 14.

Suggested Criterion - Monitoring Engineered Safety Features

We suggest that this criterion be inserted at this point: Instrumentation shall be provided to monitor the performance of engineered safety features during the course of the accident and to monitor the condition of the reactor itself under these conditions.

Criterion 16 - Monitoring Reactor Coolant Pressure Boundary

This criterion defines the monitoring that is necessary to prove compliance with Criterion 9. (Similar proof is required by Criterion 36) In cases of this nature cross referencing of criteria should be made for the sake of clarity.

Criterion 17 - Monitoring Radioactivity Releases

This criterion was written to specify monitoring to meet the specifications of Criterion 70, which should be cross referenced here.

Criterion 18 - Monitoring Fuel and Waste Storage

Specification of criticality monitoring should be included in this criterion; for example, as by reference to 10 CFR, Part 70.34.

Criterion 19 - Protection Systems Reliability

There is no guide for determining whether or not the functional reliability and in-service testability is commensurate with the safety functions to be performed. Every designer could claim that his system met this criterion, and challenge a reviewer to show otherwise. Arguments about this criterion most likely will include comparisons to somewhat similar protection systems for somewhat similar nuclear power plants that have been reviewed and approved.

This criterion is of questionable value and we recommend its omission. A set of rules for designing protection systems would be more useful than a general statement of desirable results.

Criterion 20 - Protection Systems Redundancy and Independence

The criterion is not clear as to the extent of the effects of a single failure that need consideration. Apparently, considerations of effect are to be limited to a component or channel - resulting in a severe limitation in the value of this criterion. This is another example of a criterion where definitions are needed; for example, component, channel, and system need to be defined.

Criterion 21 - Single Failure Definition

A judgment of the extent of failures caused by a single event hinges on credibility. First, there is the probability of the initiating event, then the probability of progressive failures. A single event of sufficient magnitude will certainly prevent the functioning of the protection system. Detailed guidelines for describing the required independence of redundant equipment are needed. Examples are spacing between cables carrying redundant signals, methods of separating electronic equipment handling redundant signals, methods of isolating redundant logic devices which combine redundant signals, etc. Unless more detailed information is given as to what is to be considered credible, this criterion serves little purpose.

Criterion 22 - Separation of Protection and Control Instrumentation Systems

This criterion apparently recognizes the need for separating protective and control instrumentation but compromises this objective with the qualifications permitted. The net effect is to permit the intimate intermingling of the system that normally operates the plant and the system that is intended to afford protection. We strongly recommend that no exceptions be permitted to the separation of these two systems as the only effective means to insure the vital integrity of the protection system.

Both of these systems in the new and larger reactors are complex. Despite the use of buffer amplifiers in attempting to isolate the effects of failures in the two systems, the systems are not independent when the same signals are coupled into each. Additionally, the objectives of operation are not those of protection. When the two systems are intermingled, signal processing equipment is invariably designed for operating the plant rather than for protection. Inadequate control demands that corrections must be made in the equipment to allow operation, but inadequate protection equipment may be discovered only after their need during an accident. Mixing of the two systems as allowed by this criterion diverts design attention from the requirements of protection to those of operation. Such mixing also increases the probability that protection will be lost as the result of a failure in the control system that initiates the accident requiring protection.

The basic justification for independence of protection and operation systems, in our opinion, is the relative ease with which the protection function can be assured with independence, and the great difficulty of realizing such assurance with interdependence. We believe it is easier to separate the systems than to assure that their interactions are harmless. We believe it is easier to maintain independence than to insure, for the lifetime of the plant, that deliberate changes or inadvertent alteration of the operation system will not adversely affect the protection function.

The dismal list of accidents caused by design errors, and the much larger list of design errors caught before they caused accidents, lead us to believe that design errors will continue to occur. We believe further that independence of operation and protection is one of the best defenses against the possibility that a design error may cause an unprotected accident.

It may be possible that for some combinations of protection and operation instruments no conceivable failure of the operation function involved can result in a situation requiring action of the protection function involved. To the extent that this can be proved, both initially and throughout reactor lifetime, the particular interdependence could be acceptable. A hypothetical example is the instrumentation used to measure and control the pressure of a sealed containment enclosure. The operation function is used principally to provide a pressure differential between the inside of the containment and the outside, and thus to provide a means for surveillance of the leakage rate.

The protection function might be to initiate reactor shutdown, emergency cooling, and isolation of process piping if a rise in containment pressure should indicate the presence of a serious leak of potentially radioactive fluids. It might be demonstrable that no failure whatever of this instrumentation could induce a substantial leak of radioactive fluid, in which case no real interdependence of operation system and protection system would in fact exist.

The basis of the above example is the impossibility that failure of the operational function or equipment could ever, under any circumstances, lead to a situation where the protection function would be needed. Therefore, sharing of equipment (common elements) between the protection system and the operation system could not lead to interaction between the two systems. It is difficult to prove conclusively this lack of functional interaction. More difficult is the problem of ensuring that this lack of interaction can and will be maintained throughout the life of the plant. Operators are not designers; operators in charge of the plant at the end of its 40-year life are not the ones who may have discussed protection problems with the designers at the beginning. Subtle considerations are apt to be forgotten or ignored. It is easy to forget that plant protection was originally based on the impossibility that failure of certain operation instruments could result in a need for protection-system function.

Criterion 24 - Emergency Power for Protection Systems

Design requirements related to power supply include consideration of both Criteria 24 and 26. There is an anomaly here in that Criterion 24 permits the protection system to require power to provide protection, whereas Criterion 26 requires the system to fall into a safe or tolerable state on loss of power. To the extent that Criterion 26 can be met, alternate power sources become an economic or operational consideration rather than being needed for safety.

Criterion 25 - Demonstration of Functional Operability of Protection Systems

We agree with the intent of this criterion but suggest that the wording be changed to state ". . . demonstrate that no failure causing a reduction of redundancy . . ." rather than ". . . demonstrate that no failure or loss of redundancy . . .". Some systems may have extra elements whose failures do not reduce the redundancy claimed for the system.

Criterion 26 - Protection Systems Fail-Safe Design

This criterion places a requirement not only on the protection system but on the plant as well. For example, a plant design could be such that operation of the protection mechanism when not needed would be highly undesirable. (An illustration is the closure of the steam stop valves in a

BWR.) Criterion 26 requires the plant to be able to accept operation of the protection system when not needed. We believe this is a good objective and we support this criterion.

Section V - Reactivity Control

1. The title of this section should be "Reactivity Control for Reactor Shutdown".
2. This group of criteria should distinguish more clearly between functions of reactivity control; namely, the dynamic reactivity reduction process and the static holddown functions. The first function must be performed at such times as in power transients and loss-of-coolant accidents with the objective of preventing exceeding "acceptable fuel damage limits" referred to in Criteria 28 and 29. Margins expressed in terms of shutdown parameters are inappropriate and inadequate for the dynamic function.

The reliability with which each function must be carried out depends upon the seriousness of the consequences of failure of that function.

Criterion 27 - Redundancy of Reactivity Control

This criterion is not clear. It does not state whether the two reactivity control systems (1) should both be capable of both increasing and decreasing reactivity for operation, or (2) should both be capable of fast shutdown, or (3) should one be for fast shutdown and one for holddown. We recommend that the word "shutdown" be substituted for "control" in this criterion. These systems should also meet the requirements of Criteria 28, 29, 30, 31, and 32.

Criteria 28, 29, and 30 taken together indicate that one of the shutdown systems is not required to cope with positive transients and is essentially a method of obtaining reactivity holddown capability. However, reactors that must be shut down rapidly to allow the containment system to function need two separate and fast shutdown systems. A single fast or "primary" shutdown system together with a "holddown", or slow, "secondary" shutdown system is not satisfactory in this case.

Criterion 29 - Reactivity Shutdown Capability

As stated in our comments on Criterion 27, some reactors require a shutdown to allow the containment to function. In such cases, this criterion

should require that two shutdown systems be applied. Each such system should be capable of preventing an unacceptable situation.

This criterion carries a reference to shutdown margin that could well be made a separate criterion as the shutdown requirements are a function of the number of rods, reactor operating conditions and function desired (e.g., reduction of nuclear power level or holddown of the subcritical reactor). Although we have not addressed ourselves to these conditions in detail, we believe that a margin much greater than the worth of the most effective control rod is needed for reactors having many rods.

Criterion 30 - Reactivity Holddown Capability

In cases requiring the reactor to be shut down in order to achieve containment, two of these systems should be required. See comments on Criteria 27 and 29.

Criterion 31 - Reactivity Control Systems Malfunction

This criterion should be expanded to include all failures of the plant operating system that are capable of increasing reactivity. In particular this criterion should not be limited to the unplanned withdrawal of only one control rod since a failure of the control rod operating system may not be restricted to the withdrawal of only one rod. All failures that may affect the performance of the control rod operating system must be considered. Of a more general nature, all failures that can introduce reactivity increases must be considered. In addition to control rods, there are coolant temperature changes, and perhaps even void effects that need analysis.

Criterion 33 - Reactor Coolant Pressure Boundary Capability

We agree with the intent of the criterion but it is not clear what is meant by "positive mechanical means" for preventing a rod ejection. A definition is needed.

Section VII - Engineered Safety Features

With the exception of reactor shutdown systems, all other engineered safety features are discussed in this section. These are: emergency power system, emergency core cooling system; containment enclosure system, containment pressure-reducing system (including containment heat removal), and air cleaning systems.

For each of these systems, there should be criteria for design of the system and their components as well as criteria for testing and inspection.

The objective of these criteria would be clearer if each system were treated in separate subsections and the criteria for each were set up in parallel form. Thus, there would be criteria for the inspection and testing of emergency power system (now covered in only Criterion 39) as well as the inspection and testing criteria for the other engineered safety features. Criterion 52, "Containment Heat Removal Systems," would be grouped with Criteria 58-61 with which it is generally associated. Such a rearrangement raises questions on other points of apparent inconsistency, e.g., Criterion 60 is seen to be but a special case of Criterion 61, etc.

Criterion 37 - Engineered Safety Features Basis for Design

Again a definition of engineered safety features is necessary. For example, if the scram must work in order that the containment not be overstressed, then the scram system must be considered part of an engineered safety feature.

Criterion 38 - Reliability and Testability of Engineered Safety Features

We agree with this criterion. However, its title and inclusion in Section VII, both of which pertain only to engineered safety features, does not reflect its more general applications which include "inherent" as well as "engineered safety features". It would more appropriately be included in Section I.

Criterion 39 - Emergency Power for Engineered Safety Features

A difficult point in the application of this criterion is that of redundancy in the offsite power system. For example, a plant failure that results in shutting off the electric generator driven by the reactor could produce the loss of all offsite power. The probability of this consequential loss of offsite power varies widely as a result of changes in the power system and of variations in power system load. As a result of this wide variation in the reliability of offsite power, we recommend that this criterion require that redundant and independent onsite power system be required such that onsite power alone be capable of supplying the needs of the engineered safety features after a failure of a single active component in the onsite power system. We do not believe that the offsite power is really independent of the power from a main generator operated from the reactor to be safeguarded.

Criterion 40 - Missile Protection

Analysis shall be made to show that fragments and components that could be ejected from highly pressurized system's rotating equipment would not

impair the function of an engineered safety feature. Typical missiles requiring analyses are such items as primary system valves, flanges, instrumentation, etc. When rotating equipment is not completely contained, such as in a concrete vault, a missile map should be provided for rotating equipment (e.g., main turbines, pumps, etc.)

Criterion 41 - Engineered Safety Features Performance Capability

We agree with this criterion as far as it goes. In particular the detailed requirements for the emergency core cooling system as contained in Criterion 44 illustrate the desired amplification (but for that system only). Thus, it could be generalized and added to Criterion 41 as follows: "The performance of each engineered safety feature shall be evaluated conservatively in each area of uncertainty. The systems shall not share active components and shall not share other features or components unless it can be demonstrated that (a) the capability of the shared feature or component to perform its required function can be readily ascertained during reactor operation, (b) failure of the shared feature or component does not initiate a loss-of-coolant accident, and (c) capability of the shared feature or component to perform its required function is not impaired by the effects of a loss-of-coolant accident and is not lost during the entire period this function is required following the accident."

Criterion 42 - Engineered Safety Features Components Capability

We see no need to limit this criterion to the loss-of-coolant accident and suggest that . . . "by the effects of a loss-of-coolant accident" be changed to read "the effects of the accident for which the function is required."

Criterion 43 - Accident Aggravation Prevention

It is not obvious what purpose this criterion is intended to serve. If something specific is in mind here it should be stated, i.e., are we worried about the core becoming critical again, or inducing a thermal shock, etc. Perhaps this should not even appear here but be in the general discussion.

Criterion 44 - Emergency Core Cooling Systems Capability

As noted in the discussion on Criterion 41, we would restrict this criterion to the first two sentences (having already included the remainder of this criterion as a general requirement in Criterion 41). However, as we interpret the intent of these sentences, each of the two emergency cooling systems should cover the whole range of pipe break conditions up to the

maximum. To make this point clearer, it might be better to rephrase the second sentence defining the cooling system requirements as follows: "For each size break in the reactor coolant pressure boundary, including the double-ended rupture of the largest pipe, at least two emergency core cooling systems, preferably of different design principles and each with a capability for accomplishing abundant emergency core cooling, shall be provided."

Criterion 48 - Testing of Operational Sequence of Emergency Core Cooling Systems

We agree with the intent of this criterion and suggest that in addition to "the transfer to alternate power sources" the operation of the reactivity control system (which must shutdown the reactor and then provide holddown in the cold condition after the loss-of-coolant accident) should be mentioned.

Criterion 49 - Containment Design Basis

We agree with the intent of this criterion but feel that the following need some elaboration:

Line 10: "Considerable Margin" should be defined in some manner.

Line 13: What degree of failure of the emergency core cooling system is assumed?

Criterion 50 - NDT Requirement for Containment Material

This criteria needs further clarification. The temperature of the steel members in question under normal operating and testing conditions should be defined, i.e., the temperature of the component when the ambient temperature is at its lowest recorded (or perhaps expected) value. Furthermore, the requirement of NDT + 30° F has no meaning in the eyes of the stress analyst although it has found some usage. This temperature is half way between NDT and FTE and unless there is adequate justification of which we are unaware, we recommend using NDT + 60° F which defines the transition, e.g., temperature at which cracks won't propagate at stresses less than yield.

Criterion 51 - Reactor Coolant Pressure Boundary Outside Containment

The intent of this criterion is not clear. It would appear that Criterion 53 which requires redundant valving would also cover reactor containment coolant boundaries outside containment. If, however, it is intended to require extensions of the containment, it should be specifically stated. In

any event . . . delete "appropriate" and "as necessary" in lines 4 and 5 and the entire last sentence which begins, "Determination of . . .". These words do not materially contribute to the sense of the statement of the criterion and therefore should be omitted.

Criteria 54, 55, and 56 - Containment Leakage Rate Testing, Containment Periodic Leakage Rate Testing, and Provisions for Testing of Penetrations

Following the words "design pressure" it is suggested that "defined by Criterion 49" be inserted.

Criterion 56

This criterion is not sufficiently inclusive. The types of penetrations which should be tested should NOT be limited to the two that are mentioned, but for instance should also include electrical penetrations and piping penetrations that do not require expansion joints. The penetration testing is usually done at greater than design pressure.

Criterion 66 - Prevention of Fuel Storage Criticality

We do not understand the implication of "or processes" at the end of the first sentence, nor do we believe that it is practical to depend upon procedural controls to prevent accidental criticality in storage facilities of power reactors. Hence, the last sentence of this criterion should be changed to read as follows: "Such means as geometrically safe configurations shall be used to insure that criticality cannot occur."

Criterion 67 - Fuel and Waste Storage Decay Heat

To the extent that removal of decay heat is a function necessary to prevent escape of fission products, decay heat removal systems should be designed to the same requirements for redundancy, inspectability, and testability as engineered safety features on reactors. This should include facilities for supplying additional coolant fluid in the event of accidental loss.