August 17, 1977

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

SECY-77-439

INFORMATION REPORT

FOR: The Commissioners

THRU: Lee V. Gossick, Executive Director for Operations

FROM: Edson G. Case, Acting Director, Office of Nuclear Reactor Regulation

SUBJECT: Single Failure Criterion

PURPOSE: To inform the Commission of the present status and future use of the Single Failure Criterion as a tool in the reactor safety review process.

DISCUSSION: A memorandum from the Secretariat to the Executive Director for Operations of June 30, 1977 requested that the staff maintain its schedule to develop an information paper on the Single Failure Criterion and its application. The enclosure provides that information.

The central conclusion to be drawn from this staff work is that the Single Failure Criterion has served well in its use as a licensing review tool to assure reliable systems as one element of the defense in depth approach to reactor safety. The Reactor Safety Study indicates that its use had led to a generally acceptable level of hardware redundancy in most systems important to safety. Some problems exist in specific interpretations and applications of the Single Failure Criterion, and these are the subject of ongoing work.

As for the future, the work underway will serve to codify and make more consistent our application of the Criterion in the licensing review process. It is expected that probabilistic methods of the type used in the Reactor Safety Study will gradually come into increasing use and supplement the Single Failure Criterion.

Edson G. Case, Acting Director
Office of Nuclear Reactor Regulation

Enclosure:
Information Paper on
Single Failure Criterion

DISTRIBUTION
Commissioners
Commission Staff Offices
Exec Dir for Operations
ACRS
Secretariat

Contact:
R. Ireland, NRR
49-28084

INFORMATION REPORT

BY THE

OFFICE OF NUCLEAR REACTOR REGULATION

ON THE

SINGLE FAILURE CRITERION

1. INTRODUCTION

The Single Failure Criterion is just one of several tools applied in systems design and analysis to promote reliability of the systems which are needed in a nuclear power plant for safe shutdown and cooling, and for mitigation of the consequences of postulated accidents. It is not sufficient by itself. Rules of good design practice, such as those required by the ASME Boiler and Pressure Code, IEEE standards, quality assurance requirements and conservatively stipulated design conditions must also be utilized to ensure that high quality and highly reliable systems, components and structures are provided.

The Single Failure Criterion, as a design and analysis tool, has the direct objective of promoting reliability through the enforced provision of redundancy in those systems which must perform a safety-related function. Simply stated, application of the Single Failure Criterion requires that a system which is designed to perform a defined safety function must be capable of meeting its objectives assuming the failure of any major component within the system or in an associated system which supports its operation.

The Single Failure Criterion was developed without the benefit of numerical assessments on the probabilities of component or system failure. However, in applying the Criterion, it is not assumed that any conceivable failure could occur. For example, reactor vessels or certain types of structural elements within systems, when combined with other unlikely events, are not assumed to fail because the probabilities of the resulting scenarios of events are deemed to be sufficiently small that they need not be considered. In general only those systems or components which are judged to have a credible chance of failure are assumed to fail when the Single Failure Criterion is applied. Such failures would include, for example, the failure of a valve to open or close on demand, the failure of an emergency diesel generator to start or the failure of an instrument channel to function. A single failure can also be a short circuit in an electrical bus that results in the failure of several electrically operated components to function.

The Single Failure Criterion, through enforced provision of redundancy, does not give absolute assurance of reliability. The Reactor Safety Study (WASH-1400) indicates that application of the Single Failure Criterion to the plants that were studied did provide an acceptable degree of hardware redundancy for most systems. However, the Reactor Safety Study also pointed out that factors such as systems interactions, multiple human errors, and maintenance and testing requirements also have an influence on reliability. Such factors fall outside the scope of the Single Failure Criterion, and supplementary methods must be utilized in their study.

At the present time, the Single Failure Criterion is codified in Appendix A to 10 CFR 50 (General Design Criteria) and in Appendix K (ECCS Evaluation Models); in addition, 10 CFR 50.55a (Codes and Standards) makes mandatory the use of the ASME Code and of IEEE Std 279 which contains the Single Failure Criterion. Further interpretation and guidance on the application of the Single Failure Criterion is given in the Standard Review Plan and Regulatory Guides (e.g., Standard Review Plan Section 3.6.1 describe its application in the event of postulated piping failures outside containment, and Regulatory Guide 1.53 endorses IEEE Std 379 which describes in detail how the Single Failure Criterion defined in IEEE Std 279 is applied to electrical and instrumentation systems).

2. IMPORTANT ELEMENTS OF THE SINGLE FAILURE CRITERION

A. The Concept

In principle, the Single Failure Criterion is straightforward. Simply stated it is a requirement that a system which is designed to carry out a defined safety function (e.g., an Emergency Core Cooling System) must be capable of carrying out its mission in spite of the failure of any single component within the system or in an associated system which supports its operation. Application of the concept is complicated by the interrelationships between the various fluid and electrical systems and their supporting auxiliaries in a nuclear power plant. Furthermore, there is a need to stipulate the events and associated assumptions which must be considered during application of the Single Failure Criterion.

Application of the Single Failure Criterion involves a systematic search for potential single failure points and their effects on prescribed missions (i.e., Failure Modes and Effects Analysis). Such a search is required by our Standard Review Plan and the Standard Format for the Content of Safety Analysis Reports for specified safety systems and components. The objective is to search for design weaknesses which could be overcome by increased redundancy, use of alternate systems or use of alternate procedures.

B. Definition of Single Failure

Single failure is defined in 10 CFR 50 Appendix A As follows:

> "A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of capability of the system to perform its safety functions. "

A footnote to this definition states that "single failures of passive components in electric systems should be assumed in designing against a single failure." This means that for electric systems no distinction is made between failures of active and passive components and all such failures must be considered in applying the Single Failure Criterion. For example, short circuits in electrical cables must be considered even though a short circuit could be regarded as a failure of a passive component.

With regard to passive components in fluid systems, the footnote further states, "The conditions under which a single failure of a passive component in a fluid system should be considered in designing the system against a single failure are under development."

While considerable progress has been made in defining the nature of passive component failures which should be considered in the licensing review process, no change to the regulation has been made since 1969. In application of the Single Failure Criterion to fluid systems, Section 6.3 of the Standard Review Plan requires consideration of passive failures in the Emergency Core Cooling System during the recirculation cooling mode following emergency coolant injection, but does not define the nature of such failures. Other interpretations of the Criterion for passive components have been made on the basis of detailed engineering evaluations conducted during licensing reviews, but with some staff disagreement. For example, NUREG-0138 (Issue 7) has a detailed discussion of passive failures following a Loss of Coolant Accident, and NUREG-0153 (Issue 17) has a detailed discussion of passive type valve failures. This subject is also summarized in Section 4 below and the status of standards development pertinent to this subject is summarized in Section 6. The following definitions of single active and passive failures in fluid systems important to safety are pertinent to the discussion of the Single Failure Criterion.

C. Active Failure in a Fluid System

An active failure in a fluid system means (1) the failure of a component which relies on mechanical movement for its operation to complete its intended function on demand, or (2) an unintended movement of the component. Examples include the failure of a motor- or air-operated valve to move or to assume its correct position on demand, spurious opening or closing of a motor- or air-operated valve, or the failure of a pump to start or to stop on demand. In some instances such failures can be induced by operator error.

D. Passive Failure in a Fluid System

A passive failure in a fluid system means a breach in the fluid pressure boundary or a mechanical failure which adversely affects a flow path. Examples include the failure of a simple check valve to move to its correct position when required, the leakage of fluid from failed components, such as pipes and valves--particularly through a failed seal at a valve or pump--or line blockage. Motor-operated valves which have the source of power locked out are allowed to be treated as passive components.

In the study of passive failures it is current practice to assume fluid leakage owing to gross failure of a pump or valve seal during the long-term cooling mode following a LOCA (24 hours or greater after the event) but not pipe breaks. No other passive failures are required to be assumed because it is judged that compounding of probabilities associated with other types of passive failures, following the pipe break associated with a LOCA, results in probabilities sufficiently small that they can be reasonably discounted without substantially affecting overall systems reliability.

It should be noted that components important to safety are designed to withstand hazardous events such as earthquakes. Nevertheless, in keeping with the defense in depth approach, the staff does consider the effects of certain passive failures (e.g., check valve failure, medium or high energy pipe failure, valve stem or bonnet failure) as potential accident initiating events.

3. APPLICATION OF THE SINGLE FAILURE CRITERION

As noted previously, the events and associated assumptions which are considered in connection with application of the Single Failure Criterion must be defined for specific systems. The basic events and assumptions are defined in the General Design Criteria.

A variety of design basis events which initiate a requirement for safety system action must be considered in the overall safety evaluation of a plant. In general, each of these initiating events requires an assessment of the equipment damage that could occur as a direct consequence of the event. The Single Failure Criterion is applied to those systems which must function after consequential equipment failures have been taken into account.

The General Design Criteria make it clear that for electrical, instrumentation and control systems, application of the Single Failure Criterion to systems evaluation depends not only on the initiating event that invokes safety action of these systems, together with consequential failures, but also on active or passive electrical failures which can occur independent of the event. Thus, evaluation proceeds on the proposition that single failures can occur at any time.

In contrast, for various fluid systems the General Design Criteria require that the safety function be accomplished in the face of certain conservative assumptions in addition to application of the Single Failure Criterion. In general, these assumptions involve (1) the unavailability of offsite or onsite power and (2) the postulated initiating failure. In the case of a loss of coolant accident, for example, it is first assumed that a primary system pipe rupture occurs with consequential blowdown of primary coolant.

Simultaneous with the pipe rupture, it is assumed that only the offsite power source or the onsite emergency power source is available.(1) These assumptions are applied in addition to the Single Failure Criterion which is applied to the aggregate of systems required to fulfill each specific safety function.

The manner in which the Single Failure Criterion is currently applied to various specific classes of safety related systems is outlined below.

A. Electrical, Instrumentation and Control Systems

The general interpretation and application of the Single Failure Criterion to electrical, instrumentation and control systems is stated in IEEE Std 379 as follows:

> "The system shall be capable of performing the protective actions required to accomplish a protective function in the presence of any single detectable failure within the system [this is the "single failure"] concurrent with all identifiable, but non-detectable failures, all failures occurring as a result of the single failure, and all failures which would be caused by the design basis event requiring the protective function."

---

(1) Successful emergency systems performance must be demonstrated with either offsite or onsite power, assuming a single failure.

Therefore, in the analysis to determine if a particular electrical, instrumentation or control system meets the Single Failure Criterion the following postulates are made:

(1) First, the particular design basis event or accident is postulated to occur, along with any related or consequential failures that could result from it.

(2) Then, the analysis assumes the presence of all identifiable failures which cannot be detected or tested in the design or which are not in fact subject to surveillance tests as set forth in the Technical Specifications.

(3) Finally, the presence of a single additional detectable failure is assumed in assessing the capability of the system to provide the necessary protection for the design basis event.

Analyses are performed in this manner to demonstrate the adequacy of the electrical, instrumentation and control systems design over the full range of postulated design basis events or accidents and worst case single failures.

There is a special interpretation of the Criterion (Section 4.7 of IEEE Std 279) which specifically addresses designs in which safety-related instrumentation or controls are also used to provide inputs to non-safety related plant control systems. In such a design it is required that where a single random failure in the safety-related system can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure. This special interpretation of the Single Failure Criterion is specific for the design cited above, and it is not applied to safety-related electric power systems.

The general interpretation of the Single Failure Criterion is applicable to safety-related electric power systems. However, the offsite power system is an exception. The specific requirements of General Design Criterion 17 take precedence over the rigorous application of the Single Failure Criterion; i.e., an offsite power system comprised of one delayed access circuit and one immediate access circuit is deemed acceptable. The basis for this position is that a second immediate access circuit would not significantly improve the availability of offsite power at the emergency buses. This has been established by an analysis using reliability data and not the Single Failure Criterion.

B. Emergency Core Cooling Systems

In applying the Single Failure Criterion to Emergency Core Cooling Systems which must function following postulated loss of coolant accidents, the requirements of General Design Criterion 35 - Emergency Core Cooling - are followed. Therein it is stipulated that following a postulated loss of coolant accident, suitable redundancy in equipment shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the ECCS safety function can be accomplished, assuming the most limiting additional single failure. Appendix K to 10 CFR 50 requires that the only ECCS subsystems to be assumed available are those operable after the most damaging additional single failure of ECCS equipment has taken place. Selection of the single failure to be applied to the emergency core cooling system is made independent of the size or location of the postulated pipe break in the reactor coolant system. Thus, for each postulated pipe break, that single failure which results in minimum emergency core cooling performance is considered in judging the adequacy of the system. For example, this could be failure of a component in a redundant ECCS subsystem or the loss of an emergency diesel generator in addition to the loss of all offsite power.

During the short-term ECCS coolant injection mode immediately following a loss of coolant accident, the most limiting single active failure is considered in evaluating systems performance capability.

During the long-term ECCS recirculation cooling mode the most limiting active failure, or a single passive failure equal to the leakage that would occur from a valve or pump seal failure, is assumed. The basis for not including other passive failures during the long term is based on engineering judgment that such failures (pipe or valve breaks) have an acceptably low likelihood of occurrence during the long-term phase of a loss-of-coolant accident. Analyses of ECCS performance in WASH-1400 indicate that passive failures of valves and piping are relatively small contributors to ECCS unavailability during both the injection and recirculation modes of operation.

C. Containment Heat Removal and Cleanup Systems

General Design Criterion 38 - Containment Heat Removal - requires the provision of a system to rapidly reduce containment pressure and temperature following any LOCA. While current practice is to apply only an active component failure to the evaluation of the performance of these systems, component redundancy ensures their availability even in the presence of some possible passive failures.

General Design Criterion 41 - Containment Atmosphere Cleanup - requires systems to control fission products, hydrogen, oxygen, and other substances which may be released into containment. These systems must be capable of functioning with either onsite or offsite power. Contaminants can enter the containment due to a variety of events, such as a LOCA. The Single Failure Criterion is applied subsequent to the postulated event and, in evaluating these systems, only active failures are considered, except in instances where components may be shared with ECCS systems. In such cases, the possibility of seal leakage is considered in the long-term ECCS recirculation mode.

D. Residual Heat Removal System

The capability for residual heat removal must be available using onsite or offsite power, assuming an additional single failure. To accommodate certain single failures, for the older class of plants, the staff has accepted use of the auxiliary feedwater system as a backup to the residual heat removal system. For current designs, the residual heat removal system has been modified to include additional piping and valves such that the system now has additional flexibility to perform its function even after a wide range of possible single failures. Also, as part of current staff reviews, certain initiating events have been postulated which are related to the Single Failure Criterion. These events involve application of the pipe break criteria for moderate energy lines located outside of containment as described in Standard Review Plan 3.6.1. Thus, the staff applies a limited passive failure as an initiating event for the residual heat removal system. For this event, no additional single failure is applied to the Residual Heat Removal System.

E. Ultimate Heat Sink

General Design Criterion 44 - Cooling Water - requires a system to transfer heat from systems, structures, and components important to safety to an ultimate heat sink under normal operating and accident conditions. The system must be capable of carrying out its function using either onsite or offsite power assuming any single failure. The requirements of the Single Failure Criterion are applied in a manner similar to that which is applied to residual heat removal systems.

F. Containment Piping Penetrations

Requirements for isolation valves on containment penetrations are defined in the General Design Criteria. The requirements anticipate the possibility of single active failure of isolation valves in each line by requiring double barriers. The Single Failure Criterion is also applied to the plant protection devices which initiate automatic closure of such isolation devices.

4. PROBLEMS THAT HAVE BEEN ENCOUNTERED IN THE APPLICATION OF THE SINGLE FAILURE CRITERION

A. Additional Passive Failures

As stated previously, there is a footnote in the General Design Criteria that the conditions under which single passive failures should be considered in applying the Single Failure Criterion to fluid systems are under development. That footnote was included when the Criteria were published in 1969. During subsequent years staff assumptions regarding the nature of passive failures which should be considered have not been completely consistent and there has been some disagreement. However, on the ba 's of the licensing review experience accumulated in the period since 1969, it has been judged in most instances that the probability of most types of passive failures in fluid systems is sufficiently small that they need not be assumed in addition to the initiating failure in application of the Single Failure Criterion to assure safety of a nuclear power plant. This opinion appears to have been verified by the Reactor Safety Study. Nevertheless, it is receiving further study.

In some licensing review areas, the staff does impose a passive failure in addition to the initiating event, while in others it does not. As previously mentioned, an example of the application of a passive failure requirement is the approach to long-term recovery subsequent to a loss-of-coolant accident. Applicants are required to consider degradation of a pump or valve seal and resulting leakages in addition to the initiating failure (LOCA). The rationale for applying this type of failure is a recognition of the relatively extended periods of required operation of systems that are expected to be on a standby status throughout the plant life. The likelihood of accelerated wear of such components as pump and valve seals would be increased after the adverse conditions following a LOCA. Extended operation during the long term (up to months) requires that these types of failures be considered in designing the plant. The basis for excluding additional passive piping failures is elaborated in detail in NUREG-0138, Issue 7. Other examples of passive failure considerations are presented in Section 4.B.

B. Valve Failures

A variety of valve functions and valve types exist in each nuclear plant. Valve functions include isolating flow, controlling flow, admitting flow, and preventing flow reversal. Valve types include those that are electrically controlled and operated, electrically controlled and air operated, manually controlled and operated, manually controlled and electrically operated, spring operated, and self actuated (check valves).

Accordingly, a variety of failure modes can be postulated for valves within the application of the Single Failure Criterion. Certain passive-type valve failure modes have occurred (for example, dropping of a valve disc). This has resulted in a reevaluation of postulated valve failures. NUREG-0153 (Issue 17) concludes that while the staff does not consider that changes in safety criteria are warranted at this time, ongoing efforts regarding the probability and effects of various valve failure modes will seek to compile a more rigorous data base and will apply such information to plant safety analyses. This effort has been classed as a Category B generic task.

C. Electrical Failures

In order to provide an electrical, instrumentation and control system design to satisfy the Single Failure Criterion, redundancy is included. The degree of redundancy (i.e., the number of "independent" divisions of equipment) depends on many design considerations. Provisions are typically included to prevent the initiating event from affecting the electrical, instrumentation and control systems.

If it is postulated that the failure of a portion of the safety-related electrical, instrumentation and control systems is the initiator of a design basis event, then the general interpretation of the Single Failure Criterion, discussed in Section 3.A, is not applicable to the remaining portions of the system. In such cases supplementary analyses are relied upon to evaluate the reliability of the systems in question.

In the case of the current issue on the reliability of the safety-related direct current power systems as raised by an ACRS consultant, the postulated initiating event is failure of one division of a two division system. However, this DC power system design does meet the general interpretation of the Single Failure Criterion, but it is not covered by the special interpretation noted in Section 3.A for specific safety-related instrumentation and control systems. Therefore, the staff evaluation of this issue, summarized in NUREG-0305, was based upon reliability data and not the Single Failure Criterion. It was concluded that the likelihood of occurrence of the postulated sequence of events is low enough to permit continued operation and licensing of plants pending further assessments. It is possible that new requirements to assure greater reliability of DC power systems may result from the ongoing study. It is a Category A generic task.

D. Classification of Events

Recent staff work related to issues raised in dissent or pertaining to reactor transient event classifications and consequence criteria has disclosed some confusion on how to handle certain infrequent transients which do not have public consequences as severe as "accidents". The confusion stems primarily from the differences in event classification from vendor to vendor, among standards writing bodies and within NRC. A study is underway within the Reactor Systems Branch to develop a "unified" event classification scheme. It is expected to be completed in early 1978. While this study is not aimed at application of the Single Failure Criterion, it is expected that for some events it will bring into sharper definition the circumstances under which the Criterion should or should not be applied. For example, a moderate frequency transien, such as a feedwater malfunction is routinely analyzed in Safety Analysis Reports. An additional single failure concurrent with the feedwater malfunction may result in a compound event which, because of the multiple failures, has a lower probability and therefore a different classification. Less stringent acceptance criteria may then be appropriate. The above study will examine such additional single failures as they apply to acceptance criteria for transients and accidents. This study has been classed as a Category B generic task.

E. Operator Error

An operator error could cause an active single failure, such as an inadvertent valve closure. In many instances consideration of such single operator errors is given in licensing reviews; however, the degree to which any given operator error is considered reasonably equivalent to the likelihood of a single active failure is based on judgments made concerning the situation. For example, in studying the effects of an operator error of "omission" (failure to perform an action), if there is time to bring a system on line through remedial operator action, reliance on such action is permitted. On the other hand, in cases where rapid actuation of engineered safety systems is required, the actuation is required to be automatic and operator independent.

Increasing attention is being given to human reliability in an effort to adopt more definitive criteria for the role of the operator in mitigating the consequences of transients or accidents. A Regulatory Guide is currently being developed in conjunction with staff review of the proposed Standard ANSI-N660, "Proposed ANS Criteria for Safety-Related Operator Actions." Increasing activities in human reliability will assist the staff in developing a more rigorous basis for assessing operator involvement in plant safety.

5. INSIGHTS OF THE REACTOR SAFETY STUDY RELATIVE TO THE SINGLE FAILURE CRITERION

The Reactor Safety Study (WASH-1400) assessed a pressurized water and a boiling water reactor design. The Single Failure Criterion had been applied in the design and Regulatory review processes for these plants, generally as outlined in the preceding sections. Althougn the Single Failure Criterion is not a quantitative design and analysis tool, the numerical assessments in the Reactor Safety Study indicate that its application, through enforced provision of component and systems redundancy, has made an important and necessary contribution to the overall reliability of nuclear plant safety systems. The assessments in the Reactor Safety Study also indicate that supplementary methods of analysis must be utilized to study effects on reliability which are beyond the scope of the Single Failure Criterion. The principal insights gained from this study are briefly summarized below:

(1) Application of the Single Failure Criterion has led to a suitable level of hardware redundancy in most systems. The level of redundancy thus provided has, for many safety systems, resulted in systems reliability being controlled by such factors as human and operational interactions (i.e., human errors, test and maintenance downtimes, test intervals) rather than potential single design failures as defined in the Single Failure Criterion.

Quantitative optimization of reliability in terms of such non-hardware factors would require the review of information beyond that now considered in the licensing process.

(2) The Single Failure Criterion must be supplemented by methods and criteria in the area of common mode assessments if improved reliability characteristics for safety systems are necessary. Although the effects of common mode failure are not now quantitatively considered in licensing safety reviews, considerable attention is given to reducing the potential for the occurrence of common mode failures through stringent application of high-quality design and quality assurance requirements to various components. For example, considerable attention is given to reducing the potential for multiple electrical relay failures such as might arise from a generic design defect in components supplied by a single manufacturer.

(3) The probability of accident sequences resulting in core meltdown were found by the RSS to be importantly influenced by system to system interactions and by functional dependencies between systems. These functional dependencies can be considered as a class of interactions where the functioning of one system depends on satisfactory functioning of another system. Redundancy of components within systems, mandated by the Single Failure Criterion, does not ameliorate the functional dependence. Thus, application of the Single Failure Criterion requires supplemental methods and use of an integrated systems approach to identify such functional dependencies if it is desired to further reduce accident risk.

6. ACTIVITIES RELATED TO CLARIFYING AND IMPROVING APPLICATION OF THE SINGLE FAILURE CRITERION

A number of technical activities by various nuclear industry groups and by the Offices of Standards Development and Nuclear Reactor Regulation are underway, which will have an effect on system reliability requirements and the use of the Single Failure Criterion. These are summarized in this section.

In late 1971 the American Nuclear Society initiated a standards writing effort with the objective of setting forth a clear, detailed set of criteria for application of the Single Failure Criterion to fluid systems. In 1975 the resulting Standard was issued as "ANSI N658 - Single Failure Criteria for PWR Fluid Systems." In November of 1976, the Office of Standards Development initiated a task to draft a Regulatory Guide endorsing the Standard, with appropriate exceptions, for both PWRs and BWRs. The staff review of this Standard disclosed several deficiencies which relate primarily to inconsistencies with current regulatory practice and to areas in which staff application of the Single Failure Criterion is not yet fully defined. For example: (1) literally applied to "postulated pipe breaks outside containment," the Standard would make no exception for certain dual purpose moderate energy systems (e.g., service water systems) as presently provided in Standard Review Plan 3.6.1; (2) some passive failures would be treated as active failures (e.g., check valves) contrary to staff practice; and, (3) event categorization is not consistent with current staff interpretation. Nevertheless, ANSI-N658 represents a significant step toward achieving satisfactory criteria for application of the Single Failure Criterion to fluid systems, and it is expected that a Regulatory Guide could be issued in mid-1978.

IEEE Std 379 was issued in 1972 as a Trial-Use Guide for the Application of the Single Failure Criterion to Electrical, Instrumentation and Control Systems and its application was endorsed in Regulatory Guide 1.53. IEEE Std 379 was recently updated and reissued. The subcommittee which prepared the Standard is currently working to develop definitive guidance on application of the Single Failure Criterion to shared systems and to single operator errors. When this work is completed it is expected that Regulatory Guide 1.53 will be revised to endorse these added requirements.

Earlier this year, the Office of Nuclear Reactor Regulation initiated a formal system providing for continuing management oversight and attention to generic safety-related technical activities. A number of these generic activities may include clarification of the conditions under which the Single Failure Criterion should be applied. The Category A activities expected to include single failure considerations are:

(1) Anticipated Transients Without Scram;

(2) Non-Safety Loads on Class IE Power Supplies;

(3) Adequacy of Safety-Related d.c. Power Supplies;

(4) Reactor Vessel Pressure Transient Protection;

(5) Steam Line Breaks;

(6) RHR Shutdown Requirements;

(7) Systems Interaction; and

(8) Generic Accident Risk Study

(9) Snubbers

The Category B activities expected to include single failure considerations are:

(1) Event Categorization;

(2) ECCS Reliability;

(3) Locking Out of ECCS Power Operated Valves;

(4) Protection Against Postulated Piping Failures in Fluid Systems Outside Containment;

(5) Criteria for Safety-Related Operator Actions;

(6) Passive Mechanical Failures; and

(7) Allowable ECCS Equipment Outage Periods

In some cases these activities are being conducted to evaluate adequacy of previous staff positions, while in others some new provisions may result. The single failure aspects of these activities will be utilized as appropriate in connection with improving application of the Single Failure Criterion.

The NRR staff is developing a plan for incorporating risk assessment methodology into the licensing process. Because of manpower limitations, and the need to train an initial cadre in risk assessment methodology and to carefully weigh impacts of its application, it is expected that application of risk assessment methodology to the licensing process would necessarily increase gradually over a period of several years. It is not expected that risk assessment methodology will come into large-scale systematic use in the near future as a replacement for the Single Failure Criterion as it is now applied. It is expected, however, that reliability engineering and probabilistic methodologies, together with an expanding data base on component and systems failure rates, will be applied to specific studies pertaining to reliability requirements and evaluations that go beyond the Single Failure Criterion. The current study of the adequacy of DC power supplies is an example of such an application.

7. SUMMARY CONCLUSIONS

Application of the Single Failure Criterion as it is presently defined in the regulations, Standard Review Plan, and various Regulatory Guides and industry standards has led to a generally acceptable level of hardware redundancy in most electrical, control and instrumentation systems and in fluid systems important to safety. As indicated by the Reactor Safety Study, systems unavailabilities are controlled to a large extent by factors such as operator errors, systems interactions, and maintenance and testing requirements, rather than by inadequate hardward redundancy. Some problems exist in specific interpretations and applications of the Single Failure Criterion and these are receiving staff attention. It is the considered judgment of the staff that the Single Failure Criterion should continue to be applied subject to resolution of specific problem areas currently defined and under study, pending any long-term wide-scale incorporation of reliability and risk assessment methodology into the licensing process.