Safety Classification of Electrical Safety Related Systems in Nuclear Power Plants

Electrical safety related systems in nuclear power plants today are tasked with having to meet Class 1E criteria regardless of their relative importance to safety. This one and only set of electrical safety related criteria presents a problem to the nuclear industry due to the current licensing atmosphere which has redefined safety related to include far more than just safety systems. This was originally brought to light in the issuance of the NRC Standard Review Plan (SRP) section 7.1 where safety related systems was defined to include the basic safety system, the auxiliary supporting systems and other systems important to safety. The first two categories are consistent with the industry's interpretation of those systems which are safety related and are those systems to which the Class 1E criteria apply. The third category, "other systems important to safety", has been further defined in SRP 7.1 to include " ose systems which operate to reduce the probability of occurrence of specific accidents, or to maintain the plant (including other safety s_stems) within the envelope of operating conditions postulated in the accident analyses as being required to assure full protection capability". This definition is sufficiently generic to permit the classification of all nuclear related electrical systems as safety related systems thus requiring the application of Class 1E criteria to these systems.

Class 1E criteria are not intended to be applied in toto to "other systems important to safety". On the other hand, no other electrical safety related criteria exist and the NRC is apparently not satisfied with the application of selected Class 1E criteria as deemed appropriate by good engineering judgement. It is for this reason that the industry must provide the rationale which will enable defining various classes of electrical safety related systems and the application of selected or modified Class 1E criteria to these systems. Combustion Engineering has defined

three electrical safety classes based upon identifiable categories of relative importance to safety of electrical equipment and instrumentation. The rationale for the development of these safety classes and their definitions is provided as an attachment to this letter. The application of specific Class 1E criteria is generalized as table 1 of the attachment. The electrical safety related systems which are to be classified are also generalized as those included in section 7 of an SAR. Further development of the specific criteria and the classification of systems is necessary to complete the needed safety class structure.

The insipient application of the safety class criteria proposed herein can be initiated by an interim selective criteria program. A selective criteria program can best be explained with the following example.

A typical Class 3E System might be a controlsystem which maintains reactor coolant system parameters within their operating limits. If a failure of this control system does not cause an event which, in itself or combined with other events results in an event(s) not considered in Section 15 of the Plant Safety Analysis Report, then the application of prudent engineering judgment and hardware quality commensurate with the system's function will suffice as design criteria. If a failure is postulated, however, which interacts with the protective function to the extent that it precludes completion of the required function, then the application of Selective Class 1E Criteria is necessitated (i.e., isolation and separation to assure that a fault will not propagate among control channels avoiding the spread of the fault among the Class 1E System Channels.

Safety Class 1E, 2E and 3E

The rationale for the categorization of electrical safety related systems into Class 1E, 2E or 3E systems as well as the definition of the safety classes is provided herein.

Electrical safety related systems perform a variety of functions to which the relative importance of the function with regard to plant safety varies. Those systems whose functions are most readily identifiable as existing as separate entities among the variety of functions performed include: 1) systems which directly perform protective functions (Class 1E systems), 2) systems which perform a passive safety function of preventing actions which could otherwise result in events not accommodated by the Class 1E systems, and 3) systems which perform lesser important functions such as: (a) those which provide information on plant status relative to operating limits and limiting conditions of operation. (b) those which serve to automatically control plant parameters within the operating limits and limiting conditions for operation, and (c) those non-Class 1E systems whose failure may cause an event which in itself or combined with other events results in an event(s) not considered in section 15 of the plant safety analysis report.

Designing a nuclear power plant on the basis of meeting its performance requirements (rated power, load rejection, maneuvering, etc.) without regard to consideration of equipment failure would result in the design of basic systems. These are known as non-safety systems. The need to address safety then results in the addition of safety systems, supporting systems, and safety related systems. To apply Class 1E criteria to all the systems related to safety is an extension of the purpose of the Class 1E documents and is not in recognition of the role the various systems perform in the operation of the plant. For the reasons stated above, the following

three classifications of safety related systems are provided along with the generalization of existing Class 1E criteria as might be applicable to Class 2E and 3E systems. The systems which might apply to the three categories are also generalized as those included in section 7 of an SAR.

Class 1E (IEEE 308-1974)

The classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, containment and reactor heat removal.

SRP 7.1 defines "basic safety system" as systems that directly perform a protective function (e.g., reactor trip system, emergency core cooling system, containment isolation and containment spray).

SRP 7.1 defines "auxiliary supporting system" as systems that must function to enable operation of basic safety systems (e.g., component cooling, service water, ventillation, and electric power systems which serve reactor trip system and engineering safety features).

The applicable sections of the Standard Format are 7.2, 7.3, 7.5, and 7.6.

Class 2E

Systems that are intended to protect other systems essential to reactor safety from damaging transients during normal operation and accident conditions (e.g., cold water interlocks, refueling interlocks and interlocks to prevent overpressurization of low pressure systems).

The applicable section of the Standard Format is 7.6.

Class 3E

The classification of electric equipment and systems which are provided for use in (1) indicating and/or maintaining the status of the plant relative to the operating limits and limiting conditions for operation defined in the accident analysis as required to assure full protection capability, (2) non-safety systems whose failure

could result in events not considered in Section 15 of the Safety Analysis Report.

The applicable sections of the Standard Format are 7.4 and 7.7.

Systems classified as Class 1E, 2E, or 3E may include integral parts of a system or components of a system which are of a different safety class.

TABLE 1

Standards Criteria	Electrical Safety Classes 1E	2E	3E
Seismic		As required by system's function.	As required by system's functio
Environmental	Yes	As required by system's function.	As required by system's functio
Q.A.	Yes	Yes	Yes
Single Failure	Yes	*Yes to lesser degree.	No
Electrical Separation	Yes	*Yes to lesser degree.	No
Physical Separation	Yes	*Yes to lesser degree.	No
Standby Power	Yes	*Yes to lesser degree.	No
Color Coded	Yes	*Yes to lesser degree.	No
Capability for Sensor Check	Yes	Yes	Yes
Capability for Test and Calibration	Yes	Yes	Yes
Indication of bypasses	Yes	*Yes to lesser degree.	No
Manual Initiation	Yes	As required by system's function.	As required by system's functio

---

* to the extent required to assure that acceptable reliability of performing system function** can be demonstrated. This should include consideration of the effects of the administrative controls, operating restrictions, activation of alternate or supplemental equipment and other factors that increase the probability of performin the required system function.

** preventing actions that would otherwise result in events not accommodated by the Class 1E systems.

Further clarification of "As required by system's function", "Yes to a lesser degree", "No" as applied to Class 3E and "Yes" as applied to sensor check, test and calibration and QA is provided below.

As Required by System's Function

If a Class 2E or 3E system can be postulated to fail such that its failure alone or concurrent with other events can result in an event not considered in the design basis of the safety system, then the degree of the criteria applicable to the Class 2E or 3E system would be whatever is necessary to assure that the failure or combination of failures does not occur.

Yes to a Lesser Degree

Consideration of administrative controls may include the establishment of operating restrictions or the activation of supplemental equipment. For example, a system fails resulting in a condition such that it no longer affords the degree of protection desired (testing reveals a cold water interlock inoperable). This failure presents no active threat to equipment or personnel safety; thus, it is deemed acceptable to 1) establish an operating restriction such that should the event occur, the consequences are acceptable, 2) provide an alternate means of protection (e.g. rack out the reactor coolant pump breakers), or 3) provide supplemental equipment to back up the failed system. The basis for the acceptability of this approach is the less severe consequence of the immediate failure.

"No" as Applicable to Class 3E

Not applying the criteria to which "No" applies is deemed acceptable in light of the consequences of the failure of the Class 3E system. Should a Class 3E system fail, adverse consequences are minimized by operator action. For example, the failure of the reactor regulating system to function automatically requires the operator to take manual control of the system. Administrative controls assure that LCO's are maintained. Should a Class 3E system fail concurrently with the occurrence of another event, the parameters being maintained were within their LCO's at the initiation of

the event, thus, the requirements of the safety analysis are maintained.

"Yes" as Applicable to Sensor Check, Test and Calibration and QA

The degree of the criteria applicable are, as a minimum, those necessary to assure that the systems meet their design requirements.