CRITERIA FOR SAFETY RELATED ELECTRICAL EQUIPMENT FOR NUCLEAR POWER GENERATING STATIONS

1. Scope

These criteria establish minimum requirements for the safety-related functional performance and reliability of electrical equipment for stationary nuclear reactors producing steam for electric power generation. For purposes of these criteria, the nuclear power generating station safety related electrical equipment encompasses the following:

Safety Class 1 Electrical Equipment would apply to any electrical equipment contained in an electrical system the failure of which could cause an ANS Condition III or Condition IV loss of reactor coolant. There is no electrical equipment in Safety Class 1 and, thus, requirements for Safety Class 1 Electrical Equipment have not been developed.

Safety Class 2 Electrical Equipment applies to the electrical equipment:

a. That is required to perform these safety system functions: shutdown the reactor, isolate the reactor containment, cool the reactor core, cool the reactor containment, maintain hydrogen inside the reactor containment to within acceptable limits, and maintain radioactivity inside or outside the reactor containment to within acceptable limits.

b. That is provided in the way of interlocks to prevent an operator error which could lead to a Condition III or IV accident.

c. That is required to maintain the plant in a safe and secure shutdown condition.

d. That is required to enable the operator to take manual action essential to safety during the course of an accident or during post accident control.

e. That is required to remove decay heat from spent fuel.

f. That is required to provide and distribute energy for the functions of Items a through e above.

Safety Class 3 Electrical Equipment applies to the electrical equipment not in Safety Class 2:

a. That is required to verify that plant operating conditions are within limits assumed for the safety analysis of the plant.

b. That is required to indicate the status of safety system bypasses that are not automatically removed as part of the safety system operation.

c. That is required to monitor radioactive effluents to assure that release rates and total releases are within limits established for plant operation.

2. Definitions

The definitions in this section establish the meanings of words in the context of their use in these criteria.

Electrical Equipment. Electrical equipment applies to electric motors, electric generators, and other equipment which employs electro-mechanical principles such as control rod drive mechanisms, circuit breakers, and other hardware. It applies also to electrical and electronic devices and pneumatic and hydraulic instrumentation and actuators necessary to the functioning of instrumentation or actuator systems.

Safety System. A safety system in these criteria is any system performing the functions listed in the Scope under Safety Class 2 item (a).

Safety Related Electrical Equipment. Safety related electrical equipment is equipment in safety classes as defined above.

Components. Items from which the system is assembled (for example, resistors, capacitors, wires, connectors, transistors, tubes, switches, springs, etc.).

Module. Any assembly of interconnected components which constitutes an identifiable device, instrument, or piece of equipment. A module can be

disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics which permit it to be tested as a unit. A module could be a card or other subassembly of a larger device, provided it meets the requirements of this definition.

Channel. An arrangement of components and modules as required to generate a single information signal to monitor a generating station condition or to generate a single signal to actuate safety related equipment when required by a generating station condition.

System. The word system refers to an assembly of electric and mechanical devices and circuitry (including sensors) involved in performing a particular safety function.

Train. A train of equipment refers to a portion of a system which is capable of independently performing a safety function at some fraction of the capability of the entire system. Redundant trains may be provided in order that the portion of a system which remains operable following the failure of one train will in all cases be sufficient to maintain applicable nuclear safety limits.

Type Tests. Tests made on one or more units to verify adequacy of design.

3. Requirements

Protection Systems are considered to be Safety Class 2 electrical equipment. The design requirements for Protection Systems are given in IEEE Standard 279-1971 "Criteria for Protection Systems for Nuclear Power Generating Stations". The requirements which follow apply to Safety Class 2 and Safety Class 3 electrical equipment other than the Protection Systems.

3.1 General Functional Requirement. The nuclear power generating station safety related electrical equipment shall, with precision and reliability, perform its safety related functions. This requirement applies for the full range of environmental and plant conditions under which the equipment has a safety function.

3.2 Single Failure Criterion. No single failure shall prevent any safety related electrical system (or combination of electrical systems) from performing its (or their) minimum safety related function. For Safety Class 3 electrical systems, the single failure criterion need not be met provided the plant can be put into a condition where the equipment lost as a result of the failure is not required. However, the reliability of the system design should minimize forced restrictions in plant operation due to a failure. For Safety Class 3 electrical systems, identified postulated single failures which could result in the loss of a safety function shall be detectable. A postulated failure mode can be made detectable by the use of appropriate alarms or by providing means for periodic testing. If alarms are used to meet this criterion, the equipment and each status alarm related to that equipment must be separate to the extent required to assure that a postulated failure cannot cause failure of both the system and the related alarm. For information systems, failures can also be made detectable by the use of redundant channels to monitor the same parameter or by the use of one channel to monitor one parameter and an appropriate backup channel to monitor another functionally equivalent parameter. In these cases, a failure can be detected by comparing one channel display against a second channel display. A single failure includes such events as the shorting or open-circuiting of interconnecting signal or power cables. It also includes single credible malfunctions or events that cause a number of consequential component, module, or channel failures. For example, the overheating of an amplifier module is a single failure even though several transistor failures result. Mechanical damage to a mode switch would be a single failure although several channels might become involved.

3.3 Quality of Components and Modules. Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.

3.4 Equipment Qualification. Type test data or reasonable engineering extrapolation based on test data shall be available to verify that safety related equipment shall meet, on a continuing basis, the safety performance requirements. Safety Class 3 equipment need not be qualified for accident environments or for seismic events provided that the plant can be put into a condition where the equipment is not required following either an accident or seismic event.

3.5 Safety System Integrity. All Safety Class 2 equipment shall be designed to maintain functional capability under extremes of conditions (as applicable) relating to environment, energy supply, accidents, and seismic events. Safety Class 3 equipment need not be designed to maintain functional capability following an accident or seismic event provided that the plant can be put into a condition where the equipment is not required following either an accident or seismic event.

3.6 System Redundant Channel or Train Independence. Redundant channels or trains of Safety Class 2 equipment that provide the same safety function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences, and to reduce the likelihood of interactions between redundant channels or trains of equipment during maintenance operations or in the event of a malfunction in one redundant channel or train. For Safety Class 3 systems where the requirements of Section 3.2 are met by the use of redundant channels or trains of equipment, the redundant channels or trains that provide the same safety function shall be electrically independent to accomplish decoupling of the effects of electric transients and to reduce the likelihood of interaction between redundant channels or trains during maintenance operations or in the event of equipment malfunction. Redundant channels or trains of Safety Class 3 equipment need not be physically separated provided the plant can be put into a condition where the equipment is not required should all redundant channels or trains be physically damaged.

In lieu of providing independent and redundant channels or trains for the performance of one safety function, an appropriate backup may be provided by another system which performs an equivalent safety function. The system used to provide the safety function and its functionally equivalent

backup system should be separate and independent to the same extent as required for redundant channels above.

3.7 Interfaces Between Equipment of One Safety Class and that of a Lower Safety Class.

3.7.1 Classification of Equipment. Equipment shall be classified in a Safety Class consistent with its most important function related to nuclear safety.

3.7.2 Isolation Devices. The transmission of signals or power from Safety Class 2 equipment to equipment of a lower safety class (including non nuclear safety equipment) shall be through isolation devices which shall be classified as Safety Class 2 and designed to the criteria applicable to Safety Class 2 equipment. No credible failure at the output of an isolation device shall prevent the equipment in Safety Class 2 from meeting the minimum performance requirements. Examples of credible failures include short circuit, open circuits, grounds, and the application of the maximum credible ac or dc potential. A failure in an isolation device is evaluated in the same manner as a failure of other equipment in Safety Class 2. The transmission of signals or power from Safety Class 3 equipment to non nuclear safety equipment need be through isolation devices only if the isolation is required to meet the criteria of Section 3.2.

3.7.3 Physical Interaction Between Equipment in Different Safety Classes. The physical location of Safety Class 2 and 3 equipment and non nuclear safety equipment must be such that any physical interaction between equipment in a lower safety class (including non nuclear safety equipment) and equipment in a higher safety class shall not prevent the equipment in the higher safety class from meeting the minimum performance requirements. The effects of physical interaction on Safety Class 2 equipment must include any interaction resulting from

applicable accidents and from seismic events. The effects of physical interaction on Safety Class 3 equipment need not include interaction resulting from accidents or seismic events provided that the plant can be put into a condition where the equipment is not required following an accident or seismic event.

3.7.4 Single Random Failure. Where a single random failure can cause a condition requiring the use of safety related equipment and can also prevent proper performance of one or more channels or trains of safety related equipment, the remaining safety related equipment shall be capable of performing the minimum required functions even when degraded by a second random failure.

3.8 Derivation of System Inputs. To the extent feasible and practical, inputs to safety related equipment shall be derived from signals that are direct measures of the desired variables.

3.9 Power Source. Safety Class 3 equipment shall be capable of operating independent of off-site power availability unless a documented design basis is prepared demonstrating that operability without off-site power is unnecessary. Safety Class 3 equipment need not be capable of operating independent of off-site power availability if the plant can be put in a condition where the equipment is not required following a loss of off-site power.

3.10 Capability of Sensor Checks. Means shall be provided for checking, with a high degree of confidence, the operational availability during reactor operation of each sensor used to provide input for any safety related electrical equipment.

This may be accomplished in various ways, for example:

1. by varying the monitored variable; or
2. by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable; or
3. by cross-checking between channels that bear a known relationship to each other and that have readouts available.

3.11 Capability for Test and Calibration. Capability shall be provided for testing and calibrating safety related electrical equipment. For equipment where the required interval between testing will be less than the normal time interval between generating station shutdowns, there shall, to the maximum extent possible, be capability for testing during power operation.

3.12 Safety Equipment Bypass or Removal from Operation. Safety Class 2 equipment shall be arranged in systems such that one channel or train of equipment can be maintained, and when required, tested or calibrated during power operation without interfering with plant operations. Safety related equipment arranged in two redundant channels or trains is permitted to violate the single failure criterion during bypass of one channel or train provided that acceptable reliability of operation can be otherwise demonstrated. The bypass time interval allowed for a maintenance operation will be specified in the plant Technical Specifications. Safety Class 3 equipment need not be provided with sufficient redundancy to allow bypass and maintenance of one channel or train during power operation provided the plant can be brought to a condition where the Safety Class 3 equipment is not needed should bypass and maintenance be required.

3.13 Access to Means for Bypassing. The design shall permit the administrative control of the means for manually bypassing safety related equipment.

3.14 Access to Setpoint Adjustments, Calibration and Test Points. The design shall permit the administrative control of access to all setpoint adjustments, equipment calibration adjustments, and test points.

3.15 Identification of Redundant Safety Equipment Trains. Safety Class 2 redundant equipment channels or trains shall be identified down to the channel or train level. Safety Class 3 redundant equipment channel or trains shall be identified down to the channel or train level if for the particular equipment involved the design basis requires physical separation of the redundant channels or trains. This identification shall distinguish between redundent portions of the safety class system. In the installed equipments, components or modules mounted in assemblies that are clearly

identified as being in a safety class do not themselves require identification.

3.16 Information Readout. One of the channels used to monitor each parameter providing the information required to perform the function listed in the Scope under Safety Class 2 item (d) shall be recorded to provide a historical record of the behavior of the parameter. The equipment used to record information need not be redundant nor meet the single failure criterion. A failure of the recording equipment should not negate the operability of the remaining portion of the information channel.

3.17 Repair of Safety Related Equipment. Safety related equipment shall be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.

Criteria for Electric Equipment

Safety Classes

	Single Failure (System Requirement)	Detectability of Postulated Failures (System Requirement)	Electrical Separation (System Requirement)	Physical Separation (System Requirement)	Seismic Qualification (Equipment Requirement)
Safety Class II	Yes	Yes	Yes	Yes	Yes
Safety Class III	No, provided the plant can be put into a condition where the equipment lost as a result of the failure is not required.	Yes	Yes, where redundancy or diversity is used to meet the failure criteria.	No, provided the plant can be put into a condition where the equipment is not required should it be physically damaged.	No, provided the plant can be put into a condition where the equipment is not required following a seismic event.

	Accident Environment Qualification (Equipment Requirement)	Quality Assurance (Equipment Requirement)	Independent of Off-Site Power (System Requirement)	Color Coded Redundancy (System Requirement)
Safety Class II	For any accident during which equipment is required.	Yes	Yes, unless reason for not is documented in design basis.	Yes
Safety Class III	No, provided the plant can be put into a condition where the equipment is not required following an accident.	Yes	No, provided the plant can be put into a condition where the equipment is not required following a loss of offsite power.	No, unless physical separation of redundant or diverse channels or trains is required.