AECL EACL

AECL CANDU EACL CANDU

Safety Design Guide

Environmental Qualification

CANDU 3

74–03650–SDG–003

REV. 5 / 93–03–10

Prepared by / Rédigé par	P.S.L. LEE	P.S.L. Lee
	Name / Department	CANDU 3
Reviewed by / Vérifié par	A.H. STRETCH	A H Stretch
	Name / Department	CANDU 3
Approved by / Approuvé par	P.J. ALLEN	
	Name / Department	CANDU 3

NOT A CONTROLLED COPY

TABLE OF CONTENTS

1. PURPOSE

The purpose of this Safety Design Guide is to describe the safety philosophy and requirements for the environmental qualification of safety related systems and components. The application of the principles outlined in this guide to equipment qualification ensures that the safety related systems will retain the capability to provide their intended safety function during events having harsh environmental conditions.

The safety concept, or safety philosophy, is described in Section 3 to provide designers with an understanding of the intent of the specific design requirements, which are stated in Section 4.

2. COMPLIANCE

Compliance with the Safety Design Guides is mandatory. A listing of Safety Design Guides is included in Appendix A. Deviations from the requirements identified in the guides may be allowed, after an appropriate internal safety review. All deviations shall be approved by completion of a Safety Design Guide Supplement, form PP-729.

The above recognizes that a safety function can be performed in several alternative ways, and that the designer shall be free to choose the most efficient and economical design. It also ensures that any such deviations are documented and checked for compatibility with the overall safety philosophy.

3. ENVIRONMENTAL QUALIFICATION PHILOSOPHY

3.1 ENVIRONMENTAL QUALIFICATION PROGRAM

Safety related systems and components which are required to perform safety functions during accident conditions must be designed to withstand the environmental conditions which occur as a consequence of the accident. Where these conditions are severe, and the equipment operability can potentially be affected by the environment, environmental qualification of the equipment must be carried out to demonstrate that the required safety function can be maintained. This is done through an Environmental Qualification Program.

The Environmental Qualification Program systematically identifies the equipment to be qualified and the conditions to be used for qualification, and provides a comprehensive set of documentation to ensure that the qualification is complete and can be maintained for the life of the plant.

The Environmental Qualification Program addresses the following aspects:

a. Events causing harsh environmental conditions are identified.

b. Systems and components required to perform safety functions during these events are identified.

c. Components that may be adversely affected by the harsh environment, and which must therefore be environmentally qualified are identified.

d. The environmental conditions, and their durations, which the component must withstand during normal plant operation and during the course of the accident are identified.

e. The safety function, the performance requirements, and the mission time are identified for the components requiring environmental qualification.

f. The components to be environmentally qualified are tested or analyzed to demonstrate that they will perform their required safety functions during the harsh environmental conditions.

g. Requirements for maintaining the qualification of the required components during construction and operation of the plant are identified.

3.2 ENVIRONMENTAL CONDITIONS

Safety related systems and components are required to perform their safety functions in environments which can be classified as either "harsh" or "mild".

Mild environmental conditions are not expected to cause failure of systems or components designed and maintained to normal industrial standards. These conditions include temperatures up to 50°C, a total integrated radiation dose of up to 2×10^4 rads, external pressure near atmospheric, and normal humidity. Qualification is not necessary for components subject to mild environmental conditions, unless severe local effects caused by a nearby component failure are identified and alternative components outside the area affected are not available.

Harsh environmental conditions are those which are expected to exceed a temperature of 50°C, a total integrated radiation dose of 2 x 10^4 rads, external pressures significantly greater than atmospheric, or a relative humidity of 100% (i.e., condensation on component surfaces is likely). For these conditions, qualification is necessary to demonstrate that the required safety function can be reliably performed.

The major events which cause harsh environmental conditions are loss of coolant accidents and steam line failures. For these events, the extent of the plant affected by the harsh environment is restricted to the specific plant areas shown in Figure 5, which are:

a. Reactor Building:

Systems and components in this area will be subject to the harsh conditions described in Figures 1, 2, 3 and 4. The condition of flooding will occur in the bottom of the building. The potential flood level is calculated to be 1.73 m and the design flood level is specified as 2 m.

b. ECC Equipment Room:

Systems and components in this area will be subject to high radiation only, with temperature, pressure, and humidity being that of a mild environment.

c. MSSV Room

The MSSV's and their associated power supplies and instrumentation will be subject to saturated steam with no radiation.

d. Turbine Building:

Systems and components in this area will be subject to a saturated steam atmosphere at low pressure with no radiation. The valves interconnecting the steam lines in this area are safety related (e.g., governor control valves), but their function is not required for events causing a harsh environment in the turbine building.

3.3 SYSTEMS PERFORMING SAFETY FUNCTIONS DURING HARSH ENVIRONMENTAL CONDITIONS

The safety related systems which perform essential safety functions during events causing harsh environmental conditions are described below.. Components of these systems must be either protected from the harsh environment, or qualified to withstand it.

A summary of the systems and major components requiring environmental qualification is shown in Table 1. This table is provided for guidance in the application of the concept described in this section, and will be subject to change or confirmation by the Environmental Qualification Program described in Section 3.1. The structures which must withstand these events are also included in Table 1 and indicated conceptually in Figure 5. |

a. Shutdown:

The reactor will be shut down by either SDS1 or SDS2, so components of both systems which are located in areas subject to harsh environment will be qualified. The normal

reactor regulating systems need not be qualified, provided that their failure would not cause the addition of positive reactivity exceeding the mitigation capability of SDS1 or SDS2. The isolating valves for the moderator purification system are qualified to ensure that moderator poison removal is discontinued after a shutdown system trip. For the case of an in-core LOCA (i.e., tube failure), the moderator liquid poison system will be qualified to add poison to the moderator through operator action.

b. Fuel Cooling:

The systems which provide fuel cooling for different events are qualified as follows:

1. Large LOCA:

The heat transport pumps are qualified to remain available for a short time period following reactor shutdown, to assist the emergency core cooling system. This also applies too (2), (3) and (4) below.

The emergency core cooling system is qualified to cool the fuel for at least four months, assisted by the steam generators for break sizes which cannot provide complete heat removal. In the long term after a LOCA, the moderator system is also qualified to remove decay heat (see (2) below). If the foregoing systems become unavailable, the end shield cooling system, after four months, is qualified to remove decay heat for at least one year, at which time repairs can be made to components in the reactor building or alternative arrangements can be made for fuel cooling. The Group 2 support services needed for operation of these systems are qualified to remain available (i.e., feedwater, electrical power, and cooling water). The liquid relief valves and pressurizer relief valves will remain available to provide overpressure protection. The heat transport pump gland seal cooling will be qualified, as necessary, to enable operation of the heat transport pumps. The fuelling machine is qualified to remain on-reactor (i.e., remains connected and motionless).

2. LOCA + LOECC:

For this event, the emergency core cooling system is unavailable, and the moderator system is qualified to provide fuel cooling following pressure tube/calandria tube contact. The Group 1 electrical system and Group 1 recirculated cooling water system supplies to the moderator system are qualified to remain available. The moderator cover gas system is designed to ensure an adequate moderator subcooling temperature by maintaining pressure on the moderator in the calandria. The hydrogen monitoring and control system is qualified to detect and control the presence of the hydrogen produced during this event.

3. LOCA + LOAC:

For this event, the local air coolers are unavailable. This results in higher temperatures and pressures in the long term, but does not affect the peak temperature and pressure. The systems and components qualified for a large LOCA are also qualified for this event.

4. Small LOCA:

   For purposes of environmental qualification, a small LOCA is considered to be a break which exceeds the makeup capability of the heat transport D_2O feed pumps. Breaks smaller than this size will cause only local effects, and will not result in harsh environmental conditions affecting other mitigating systems (also see (7) below).

   The small LOCA events include fuel channel feeder breaks and smaller breaks, for which the emergency core cooling system acting alone will not be effective for fuel cooling, due to the small break size. The fuel cooling will be provided by the steam generators, so the Group 1 auxiliary feedwater and the Group 2 feedwater system and associated level controls will be qualified for this event. Both Group 1 and Group 2 support services needed to maintain the feedwater systems (electrical power, cooling water) must remain available. In addition to the systems described in (1) above, valves on the heat transport system pressure boundary are qualified to avoid a loss of inventory in the heat transport system.

5. Main Steam Line Breaks Inside Reactor Building:

   For these events, which bound breaks of the main steam lines, feedwater line breaks, and steam generator blowdown line breaks, the steam generators provide fuel cooling. The Group 2 support systems (feedwater, electrical power) are qualified to maintain feedwater flow to the steam generators. Losses of coolant from the heat transport system will be prevented by the qualification of valves on the pressure boundary, which will either fail safe or will be closed by operator action (e.g., HT liquid relief valves, pressurizer relief valves, HT bleed valves, or alternative components). The heat is rejected through the MSSV's using Group 2 controls, which will be qualified if routed through areas subject to harsh environment. Irradiated fuel in the fuelling machine will be cooled sufficiently that fuel failure will not occur, by means of an emergency cooling supply to the F/M head from Group 2.

6. Main Steam Line Breaks Outside Reactor Building:

   For these events, which bound breaks of the main steam lines and feedwater line breaks in the turbine building, fuel cooling is performed as in (5) above. In this case, the MSSV's and their services in the MSSV room will be qualified for the resulting environment in the turbine building. For Group 1 feedwater line breaks, Group 2 feedwater is provided to the steam generators. The wall between the turbine building and the reactor auxiliary building and the Group 1 service building is designed to prevent the harsh environment from extending beyond the turbine building, ensuring that the Group 1 support services remain available. This includes electrical power supply from the grid to the Group 1 Class III buses.

7. Other:

   Heat transport system leaks, up to the capacity of the D_2O feed pumps to provide makeup, are not considered to result in a harsh environment. In general, the normally operating systems will remain available and will not require qualification, but the local effects of leaks due to component failure (e.g., instrument tube failures) will be

examined, to ensure that sufficient equipment remains available to perform the essential safety functions.

c. Containment:

The containment boundary will be maintained for all LOCA events. The containment penetrations, containment isolation components, and post-accident monitoring components are qualified or located in areas not subject to the harsh environment. For the steam line break events, a breach in the containment boundary will not result in release of radioactive materials in quantities which would cause release limits to be exceeded, but the structural integrity of the reactor building will be maintained.

d. Monitoring and Control:

The monitoring and control instrumentation required by the above systems to perform their safety function is qualified. The post-accident management instrumentation needed by the operator to monitor the state of the plant during the identified events is also be qualified.

3.4 ENVIRONMENTAL QUALIFICATION DESIGN PRINCIPLES

The design of the plant incorporates the following principles to minimize the number of safety related components which must be environmentally qualified and to simplify the process of establishing and maintaining the qualifications:

a. Areas of the plant subject to harsh conditions are minimized through the use of barriers, as follows:

   1. Harsh conditions caused by loss of coolant accidents are restricted to the reactor building and the ECC room in the Group 2 area of the reactor auxiliary building.

   2. Harsh conditions caused by steam line breaks are restricted to the reactor building, the turbine building, and the main steam safety valve room adjoining the turbine building.

b. Where practical, safety related components are located outside of areas subject to harsh conditions.

c. The number of different conditions used for environmental qualification of components are minimized by consolidating conditions created by individual events into a small number of bounding curves.

d. Safety related components are located outside of areas subject to flooding.

4. ENVIRONMENTAL QUALIFICATION REQUIREMENTS

4.1 GENERAL

a. A co-ordinated and documented Environmental Qualification Program shall be carried out to ensure that systems and components requiring qualification, including any interfacing equipment which may affect its safety function, are identified and qualified. The EQ Program shall address the requirement that qualification of required components shall be maintained during construction and operation of the plant.

b. The plant design shall consider all events which could cause harsh environmental conditions.

c. Safety related components shall be located in areas protected from harsh environments, where practical.

d. The barriers shown in Figure 5 shall be designed to prevent the propagation of harsh environmental conditions to other areas of the plant. Openings in the barriers, such as doors and ventilation ducts, shall be designed to avoid propagation of the harsh environmental conditions to areas of mild environment which contain essential safety related components. Additional barriers shall be provided, where necessary, to protect specific components from localized effects of events, consistent with the grouping and separation concepts included in 74-03650-SDG-004. The structural design of these barriers may use pressure and temperature conditions derived directly from the analysis of the relevant events, rather than the conditions identified in Figures 1 to 4 which include additional margins.

e. The designer shall ensure that equipment which performs a safety function during an event causing condition of flooding in the Reactor Building is located above the design flood level.

4.2 COMPONENTS TO BE QUALIFIED

The following steps shall be used to identify components to be environmentally qualified.

a. For each event creating harsh environmental conditions, identify the systems required to perform the safety functions of reactor shutdown, heat removal from the core, containment, plant control and monitoring, and support services. (See 74-03650-SDG-001 for a listing of safety related systems).

b. For each of the systems identified in (a), components required for performing the safety function shall be either protected from the harsh environmental conditions or shall be environmentally qualified.

c. Systems and components not required to perform safety functions during an event, but whose failure due to harsh environmental conditions could impair the safety functions of the qualified systems and components, or lead to more severe environmental conditions than those analyzed, shall also be environmentally qualified.

d. A list of systems and major components requiring environmental qualification is given in Table 1. The list is for guidance and is subject to confirmation, as required by (a) above. Designers of each system shall identify all components necessary for performing the safety functions required of each system.

4.3 NORMAL ENVIRONMENTAL CONDITIONS

Designers of each safety-related system shall establish the conditions (and the acceptable variations) under which each component of the system will be operating during normal service conditions (including temperature, pressure, radiation), including the effect of transient conditions expected to occur during the life of the plant. These conditions shall be stated in the design documentation.

4.4 HARSH ENVIRONMENTAL CONDITIONS

a. Harsh environmental conditions shall be defined as those which exceed either of the following:

1. temperatures of 50°C
2. total integrated radiation dose of 2×10^4 rads

b. The harsh environmental conditions defined for environmental qualification of components shall include those that deviate from those established for normal operation, including:

1. temperature (differential across walls or boundaries, peak, rate of change)
2. pressure (differential, peak, rate of change)
3. radiation field
4. humidity (steam environment)
5. water spray (if applicable)

c. During the event, components may be subject to additional conditions that may affect the capability to perform the safety function (depending on the nature and design of the component), including high mechanical stresses, vibrations, voltage/current surge, or chemical attack (oxidation, corrosion), and these shall also be considered in the qualification of the component.

d. The curves in Figures 1 to 4 envelope the transients predicted by analysis (see 74-03570-AR-001) for the various events. A small margin has been added as contingency to cover the possibility that future detailed analyses may yield conditions which slightly exceed those currently predicted. No margins have been added for test chamber profile requirements (e.g., to meet margin for type testing as required by IEEE-323). These bounding conditions do not necessarily include local effects which may be more severe than the average. Such local effects shall be identified by a systematic plant layout review.

e. Where the structure or component must be qualified to more than one bounding event, a composite profile shall be generated to bound the most severe conditions of each event.

f. The expected humidity conditions shall also be considered in environmentally qualifying the structure or component.

g. Where a test chamber is used, heating with steam shall be considered to most closely simulate the expected conditions.

h. The radiation doses used for qualification of components shall be derived from 74-03633-AR-001, which provides radiation dose rates for various locations for each of the major events. Beta radiation shall be considered for components or materials subject to damage by beta radiation.

i. Conditions of water immersion shall be avoided, but where such conditions cannot be eliminated by design, the component shall be qualified by testing. Oxidation and corrosion shall be considered by designers separately, wherever applicable.

j. Designers of each component requiring environmental qualification shall document the environmental conditions used for qualification of each component that performs a safety function in system design documentation. Changes in analyses, design assumptions and layout during the process of design and construction of the plant shall be monitored for deviations from the documented conditions.

4.5 QUALIFICATION OF COMPONENTS

a. For components which perform a safety function in the presence of a harsh environment, the designer shall assess whether the operability of the component could be potentially impaired, considering the minimum allowable performance. This assessment shall be done for all defined environmental conditions, including radiation, temperature, pressure, and humidity. For example, the designer shall ensure that pneumatic actuators will function under the combination of maximum containment pressure and minimum instrument air pressure. Those that could be potentially impaired during their required mission period shall be qualified by analysis, test, or demonstration of previous experience in similar environmental conditions.

b. Non-qualified components connected to or adjacent to environmentally qualified components shall be evaluated to determine whether their failure can adversely affect the safety function of the qualified component, and qualified if necessary. As a minimum, the following practices shall be used:

   1. there shall be no direct connection between qualified and non-qualified electrical circuits within the area of harsh environment, and qualified circuits shall be supplied from separate fuses or breakers, which are also qualified if necessary.

   2. environmentally qualified components that require instrument air to perform their safety function shall be provided with dedicated air receivers, or shall be designed to perform their safety function by going to a fail-safe position.

c. Guidance for acceptable qualification methods is given in Design Guide 74-30060-DG-002 and in IEEE 323 (1983): "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations". In applying the IEEE standard, it should be noted that references to seismic events should be ignored, and that Safety Design Guide 74-03650-SDG-002 shall be used instead (i.e., for LOCA + SDE), as Canadian regulatory requirements do not require consideration of a simultaneous earthquake and LOCA.

d. Type tests are the preferred method of qualification; where type tests are impractical, analysis or operating experience (or a combination of both) may be used to qualify components.

e. Qualification analyses or tests shall be documented as outlined in Section 5.

f. The event duration used to establish the mission period for systems and components shall be based on a twelve month duration for the LOCA events, and a one week duration for the steam line break events. The mission period during which individual components or systems must perform their safety function may be different than the event duration (e.g., shut-down of reactor), and if so, the mission period and any reduced environmental conditions shall be justified in design documentation.

g. For type tests, appropriate margins shall be applied to the specified environmental conditions to account for variation in production of equipment and instrument or measurement inaccuracies. Acceptable margins are given in IEEE-323. It should be noted that margins are already used in the specification of environmental conditions to cover analysis uncertainties. Engineering judgement should be used to determine that the margin is adequate for uncertainties, but not overly conservative.

h. Many non-metallic materials, particularly polymers, display aging mechanisms which are significant enough to affect their functions during the life time of the plant. In the environmental qualification of components, each functional material shall be reviewed for aging based on sample aging tests, operating experience or published test data. Where aging mechanisms are significant, they shall be considered in the environmental qualification method. Where tests are used for qualification, equipment or materials pre-aged by accelerated conditions shall be used. Where analyses are used for qualification, aging shall be based on documented test data or operating experience.

   For components with aging mechanisms, a qualified life and replacement frequency shall be established. To qualify such components to harsh environmental conditions from design basis events, they are assumed to have aged to the end of their qualified life before the design basis event occurs.

i. Certain materials show different rates of deterioration when harsh environmental conditions are present simultaneously than when these conditions act in sequence. Some materials are sensitive to the sequence of application of harsh environmental conditions. These are known as synergistic effects. At present, the only well known synergistic effects occur in the sequence of application of radiation and temperature. Materials with known synergistic effects shall be qualified for the more severe combination or sequence.

4.6 LAYOUT REVIEW OF INSTALLED EQUIPMENT

In the Environmental Qualification Program, it shall be stated that the plant owner shall establish a surveillance program to monitor qualified components for possible deterioration due to aging, including potential contributions such as storage, transportation, and installation.

A layout review (site walkdown) shall be carried out during construction/commissioning to confirm that the location and installation of the equipment conforms to the location as analyzed in the Environmental Qualification documents. Field run equipment which is environmentally qualified shall be installed according to specific procedures to maintain that qualification and shall be checked after installation for potential local effects during the layout review. The layout review team shall include the designer and members from construction and operation. The designer shall identify potential local effects during the layout review.

5. DOCUMENTATION

a. The design documentation shall identify the environmentally qualified systems, the safety functions performed, the events for which the safety function is needed, and the environmentally qualified components in each system.

b. The assessment of components to determine the need for qualification shall be included in the design documents in an auditable manner, including the reasons that qualification is not required for components which perform a safety function for events which cause a harsh environment.

c. For environmentally qualified components, the design or qualification documentation shall identify the following:

1. the location of the component;
2. the mission period;
3. associated equipment and interfaces, such as limit switches, conduit seals, electrical connections, which could affect the operation of the qualified equipment in an adverse environment;
4. the need for protection from environmental effects such as water spray or flooding;
5. the normal environmental conditions expected during normal operation of the plant (pressure, temperature, humidity, radiation or other conditions which may contribute to aging), including the duration of higher or lower conditions, (e.g. conditions during shutdowns);
6. normal equipment operating temperature and operating duty (continuous, cyclic, standby, etc.);
7. the harsh environmental conditions expected during the mission period.
8. performance requirements under accident conditions (include fluctuations of voltage, line frequency, etc.);
9. aging mechanism to be considered in the qualification, with justification;
10. the effect of unqualified systems or components which interface with the system;
11. synergistic effects to be considered in the qualification (e.g., sequence of thermal and radiation aging);
12. equipment functions to be monitored during qualification, and the minimum acceptable performance;
13. whether the test installation must be the same as the field installation.

d. The component qualification report for qualification done by test or analysis shall include:

1. description of the component and its performance specifications, or a reference to other suitable design documentation;

2. the list of materials used in the equipment, with the material specification or a reference to other suitable design documentation;
3. the acceptance criteria to indicate adequate qualification, or a reference to other suitable design documentation
4. the qualification program, stating:
   i. the normal service conditions,
   ii. the harsh environmental conditions used for qualification, and
   iii. the aging considerations, if applicable, including the radiation dose rate, aging temperature and duration, identification of activation energy (for analysis using the Arrhenius model), and any applied safety factors;
5. the summary and conclusions to show compliance with the acceptance criteria, and the qualified life of the component;
6. any supporting data;
7. a signature and date.

e. Qualification test reports shall include the information listed in (d) above, and the following:
   1. the variables measured, including accuracy;
   2. the number, type, and location (distance from sensors) of the test monitoring equipment sensors for each variable;
   3. calibration of monitoring equipment (method and date);
   4. the static and dynamic performance characteristics;
   5. any special conditions applied, such as supply voltage variations, water, etc.;
   6. the equipment mounting for the test and at the station, if relevant to performance;
   7. the cable connections and other interfaces;
   8. the test results, stating:
   9. a description of the test facility and instrumentation with calibration traceability records,
      i. the test procedure, and
      ii. the test data and accuracy;
      iii. the test failures and their resolution satisfactory to both the supplier and AECL.

f. Regardless of the method of qualification, the supplier's test qualification plan for each equipment shall receive AECL acceptance prior to the equipment qualification test. In addition, the test report for each component must be submitted to AECL for acceptance. All qualification documentation shall be handled in accordance with the Project Procedures.

g. AECL must be informed by the supplier/laboratory of any equipment failures during qualification tests. All such failures shall be analysed by the supplier to determine if the failure was a random occurrence, or caused by the environmental conditions. For random

failures, testing of equipment may be resumed with AECL acceptance. Otherwise, equipment redesign by the supplier may be necessary to eliminate such failures in the future.

Table 1
Systems, Structures and Major Components Required to Withstand Harsh Environmental Conditions

GSI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event
20000	**Buildings and Structures**		
21100	Reactor Building	To maintain an effective barrier to release of radioactive material to the outside of the building	LOCA+LOECC, LOCA+LOAC
		To prevent propagation of harsh environment to other areas of the plant	MSLB + LOAC
21130	Containment penetrations and isolation devices (to be specifically identified under process or control systems)	To maintain an effective barrier to release of radioactive materials to the outside of the building	LOCA+LOECC, LOCA+LOAC
		To prevent propagation of harsh environment to other areas of the plant	MSLB + LOAC
21160	Special Equipment (Airlocks and Equipment Hatch)	To maintain an effective barrier to release of radioactive materials to the outside of the building	LOCA+LOECC, LOCA+LOAC
		To prevent propagation of harsh environment to other areas of the plant	MSLB + LOAC
212XX	ECC Equipment Room	To prevent propagation of harsh environment (high radiation only) to other areas of the plant	LOCA
212XX	MSSV Room	To prevent propagation of harsh environment to other areas of the plant	MSLB#
22000	Turbine Building	As above	MSLB#
31700	**Reactivity control units**		
31740	Vertical flux detectors	To provide signals for reactor shutdown. (See 68000)	LOCA + LOAC LOCA + LOECC MSLB + LOAC

GSI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event
31800	**Shutdown Units**		
31810	Mechanical shutdown units	To provide reactor shutdown	LOCA+LOAC, MSLB+LOAC, LOCA+LOECC
31820	Liquid injection shutdown units	To provide reactor shutdown	LOCA+LOAC, MSLB+LOAC LOCA+LOECC
31830	Ion Chambers	To provide signals for reactor shutdown (see 68000).	LOCA + LOAC LOCA + LOECC MSLB + LOAC
31840	Horizontal Flux Detectors	To provide signals for reactor shutdown. (See 68000)	LOCA + LOAC LOCA + LOECC MSLB + LOAC
31850	Fission Chamber Units	To provide signals for reactor shutdown. (see 68000)	LOCA+LOAC, LOCA+LOECC MSLB+LOAC
32000	**Moderator system**		
32100	Moderator circulation system	To remove heat from the fuel through calandria tube-pressure tube contact.	LOCA+LOECC
		To maintain integrity so as not to drain moderator.	LOCA+LOECC, MSLB+LOAC, LOCA+LOAC
32300	Moderator cover gas, relief valves	To ensure adequate moderator subcooling	LOCA+LOECC SMALL LOCA
		To prevent radioactive release	MSLB+LOAC
32203	Purification isolation valves	To isolate purification circuit from moderator to prevent inadvertent poison removal.	LOCA+LOECC, MSLB+LOAC, LOCA+LOAC
32700	Moderator Liquid Poison System	To add poison to moderator after an in-core event.	SMALL LOCA
33000	**Heat transport system**		
33100	Heat transport system pressure boundary and isolation valves.	To maintain inventory of heat transport coolant.	MSLB+LOAC, SMALL LOCA

GSI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event
33120	Heat transport pumps	To provide forced circulation of HTS coolant.	LOCA SMALL LOCA
33140	Gland seal cooling system	To provide cooling to HTS pump seals so as to maintain seal integrity.	LOCA+LOECC, MSLB+LOAC LOCA+LOAC SMALL LOCA
33310	Pressurizer	To accommodate D_2O volume change in the HTS.	MSLB+LOAC, SMALL LOCA
	Liquid relief valves	To provide over pressure protection for the HTS.	LOCA+LOAC, MSLB+LOAC SMALL LOCA
	Pressurizer steam relief valves	As above	LOCA+LOAC, MSLB+LOAC SMALL LOCA
	D_2O Feed Pumps	To provide short term light water make-up to HTS	SMALL LOCA
33400	Shutdown cooling system*	To remove decay heat from the HTS following reactor shutdown and initial cooldown.	HTS leak** MSLB#
34000	**Auxiliary systems**		
34110	Shield Cooling System	To remove long-term decay heat from the reactor.	LOCA+LOAC, LOCA+LOECC
34320	Emergency core cooling		
	D_2O isolation valves	To supply injection of coolant to the HTS.	LOCA+LOAC
	High pressure injection	To provide injection of coolant to the HTS.	LOCA+LOAC
	Low pressure recirculation	To provide long-term coolant recirculation and heat removal to the HTS.	LOCA+LOAC, LOCA+LOECC
34700	Liquid injection shutdown system (also see 68300)	To provide reactor shutdown.	LOCA+LOAC, MSLB+LOAC, LOCA+LOECC

GSI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event
35000	**Fuel handling**		
35200	Fuel changing system	(a) To maintain pressure boundary integrity of HTS when F/M head is on reactor. (i.e., not to create a LOCA due to machine or control failures in the harsh environmental conditions). (b) When the F/M is on fuelling port, not to breach containment. (c) To cool the fuel in the F/M for events for which the containment boundary is not maintained.	MSLB+LOAC, LOCA+LOAC, LOCA+LOECC
36143	Main Steam Safety Valves*	To remove heat from the steam generators following reactor shutdown.	LOCA + LOAC MSLB#
36310	Steam Generator Blowdown System	To maintain the capability of the steam generator to remove heat from the HTS.	S/G blowdown system pipe break
43000	**Feedwater and Auxiliary Steam Systems**		
43230	Feedwater System (Group 1)	To control pressure and level on the secondary side of the SG.	MSLB (small) SMALL LOCA
	Feedwater check valve inside the R/B	To prevent outflow of water from the secondary side of the SG.	MSLB+LOAC
43300	Group 2 feedwater system	To provide water to the steam generator when Group 1 feedwater is unavailable.	SMALL LOCA, MSLB+LOAC
50000	**Electrical power systems**		
	Cables and connections Class III power (group 1)	To provide power for mitigating system (moderator) operation when Class IV power is unavailable	LOCA+LOAC, MSLB+LOAC, LOCA+LOECC
	Class II power (group 1)	To provide uninterruptible A-C power to mitigating systems.	as above

GSI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event
	Class II Power (group 1)	To provide uninterruptible D-C power to mitigating systems.	as above
	Class III power (group 2)	To provide power for mitigating system operation when Class IV power and Group I Class III are unavailable.	as above
	Class II power (group 2)	To provide uninterruptible A-C power to mitigating systems when Group 1 power is unavailable.	as above
	Class I power (group 2)	To provide uninterruptible D-C power to mitigating systems when Group 1 power is unavailable.	LOCA+LOAC, MSLB+LOAC, LOCA+LOECC
57600	Containment penetrations	To maintain an effective barrier to the release of radioactive materials.	LOCA+LOECC, LOCA+LOAC, MSLB+LOAC
60000	**Instrumentation and control**		
	For equipment inside containment only. The applicable I&C systems corresponding to the 30000 GSI series mentioned in previous pages.	To provide signals for the shutdown systems. To provide signals for control and monitoring of process and safety related systems for mitigating design basis events. For events for which these systems have no mitigating functions, qualification may be required so that failure of control will not lead to consequences beyond those analysed.	Refer to 30000 series notes.
68000	**Safety Systems**		
68200	SDS1 trip channels	To provide signals for reactor trip.	LOCA + LOAC, LOCA+LOECC, MSLB + LOAC

GSI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event
68300	SDS2 trip channels	To provide signals for reactor trip.	LOCA + LOAC, LOCA+LOECC, MSLB + LOAC
68400	Containment System:		
68430	Containment instrumentation (pressure and activity)	To provide signals for actuation of special safety systems.	LOCA+LOECC, LOCA+LOAC MSLB+LOAC
68460	Hydrogen Monitoring and Control	To provide controlled combustion H_2/D_2.	LOCA+LOECC
68500	ECC system: (see 60000)		
68930	Post Accident Monitoring	To provide monitoring of safety related systems after an event	Refer to GSI for individual systems
71310	Group 1 Raw Service Water System *	To remove decay heat, after reactor shutdown and initial cooldown, from the shutdown cooling system.	MSLB# LOCA+LOECC
71340	Group 1 Recirculated Cooling Water System*	as above.	LOCA+LOECC MSLB#
73000	**Heating, ventilation and air conditioning system**		
73111	Reactor building local air coolers	To reduce containment temperature and pressure.	LOCA, LOCA+LOECC, MSLB+LOAC
73120	Reactor Building Ventilation System	To prevent propagation of harsh environment to other areas of the plant	MSLB+Loss of containment isolation
73130	Clean Air Discharge System	as above	MSLB+Loss of containment isolation
73140	Reactor Building Containment Isolation	To provide containment isolation	LOCA+LOECC, LOCA+LOAC MSLB+LOAC

GSI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event
	Group 2 Local Instrument Air Tanks	To provide back-up instrument air supplies to qualified mitigating Systems***.	LOCA+LOAC, LOCA+LOECC MSLB+LOAC,
73230	Group 1 Service Building Ventilation System	To prevent propagation of harsh environment to other areas of the plant	MSLB+Loss of containment isolation

* Note: Systems identified by an asterisk are located in areas not affected by the harsh environment, but may have some components in the affected areas.

** Up to the capacity of D_2O feed pumps.

*** Instrument Air for Group 2 Systems is normally supplied by Group 1 Instrument Air (75120).

Outside of the Reactor Building, use specific conditions for that location.

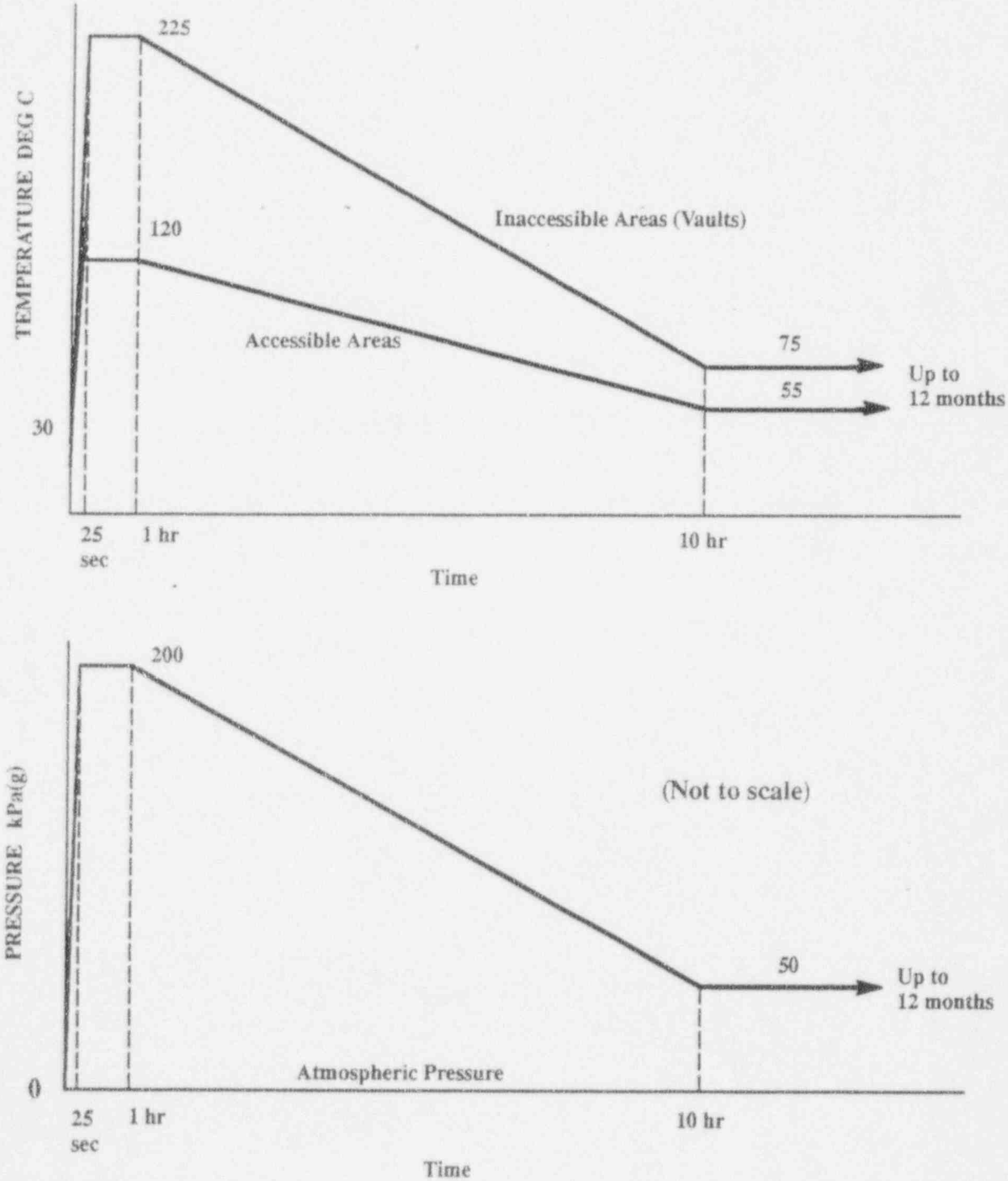
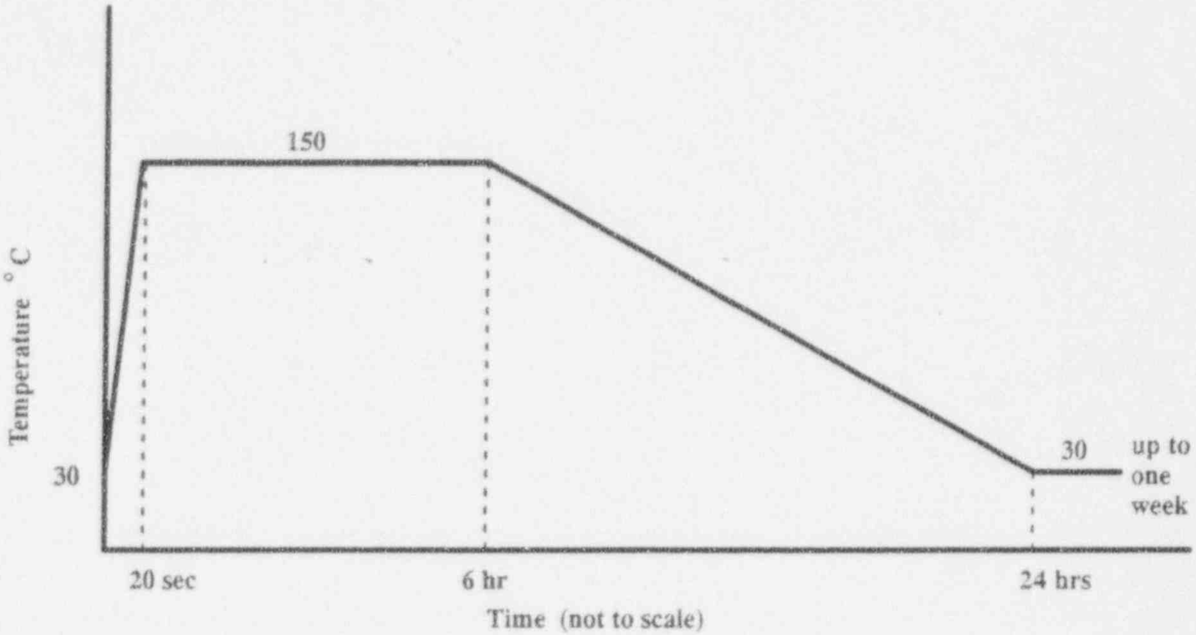
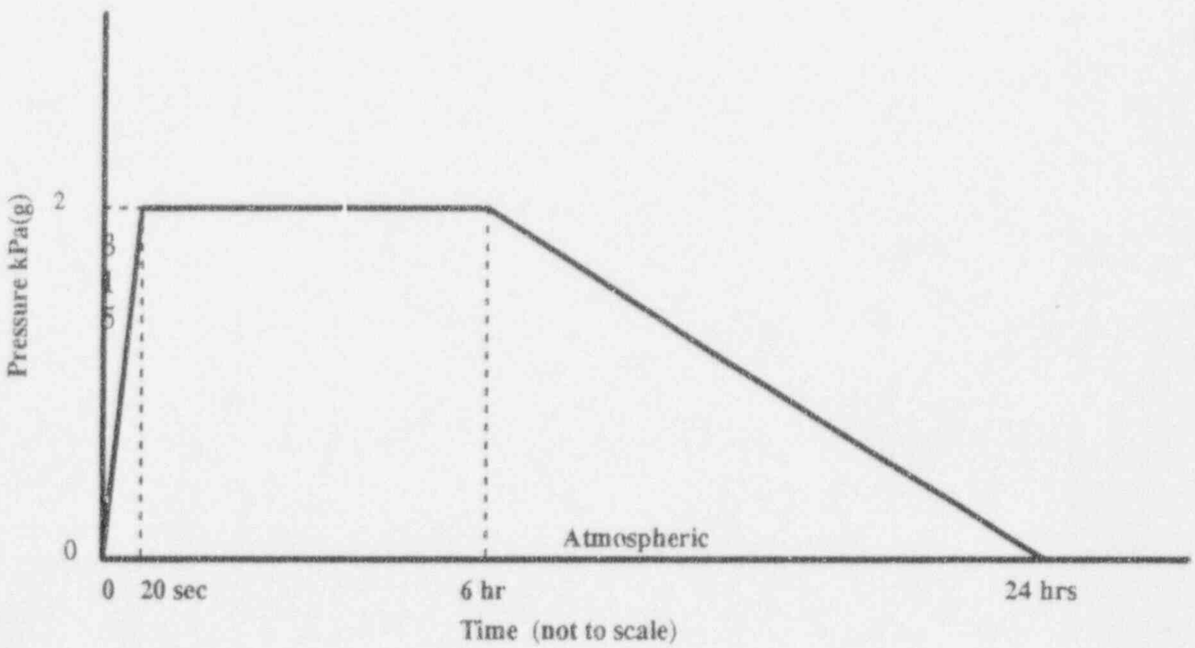


FIGURE 1 ENVIRONMENTAL ENVELOPES FOR LOCA, LOCA + LOAC, and LOCA+LOECC

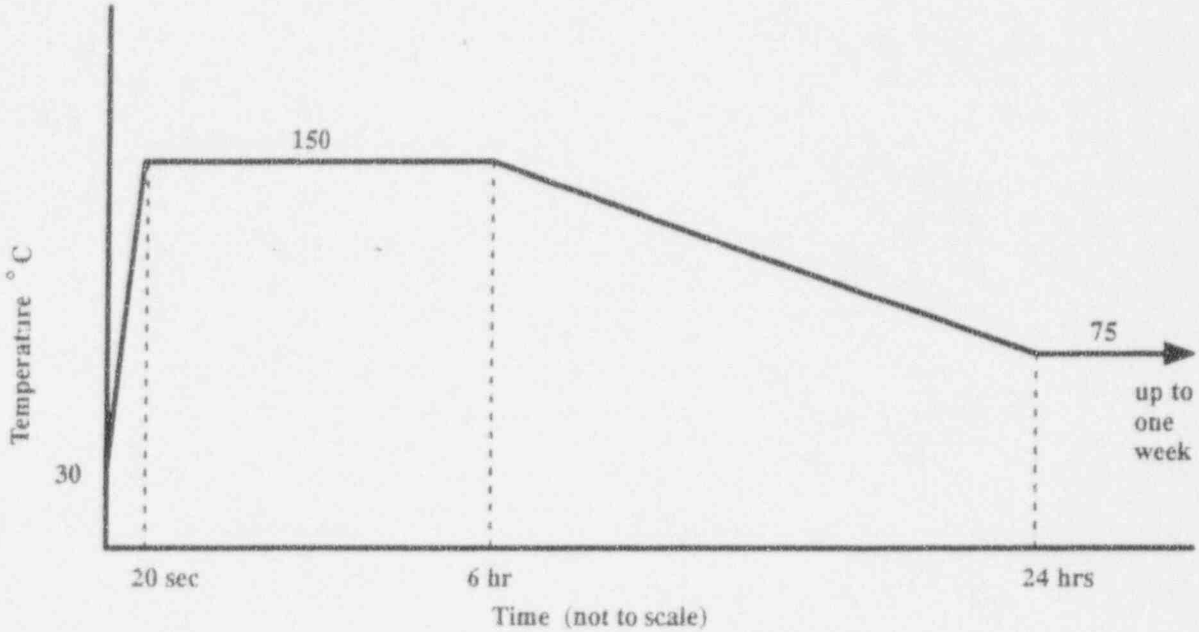


TEMPERATURE ENVELOPE

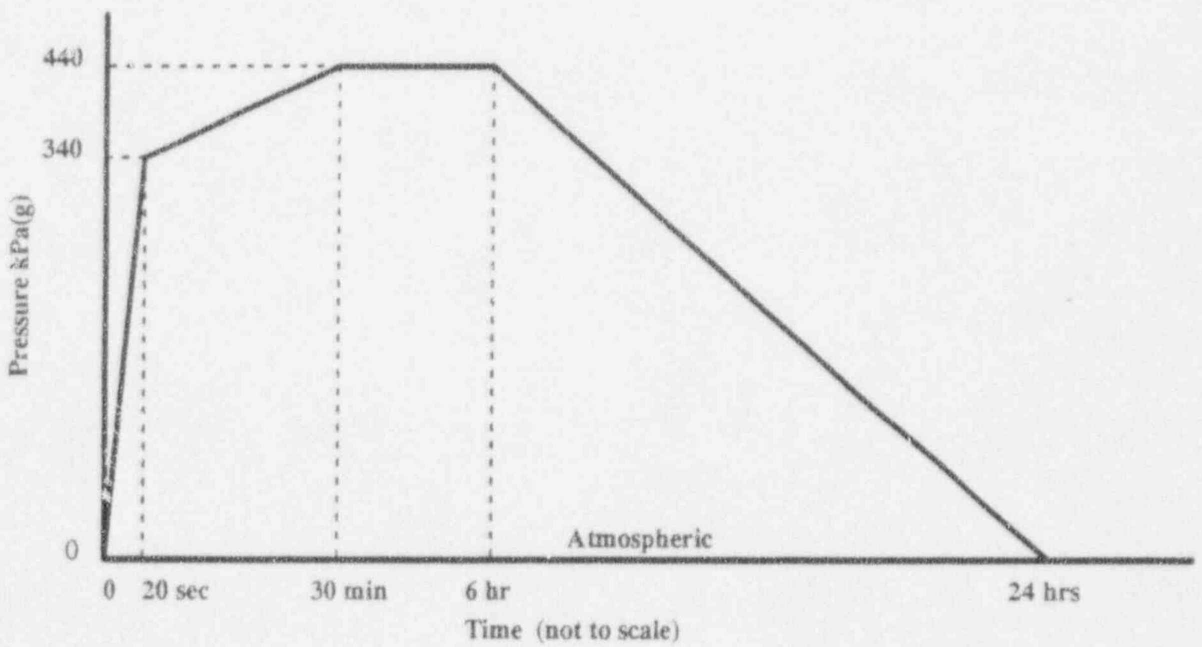


PRESSURE ENVELOPE

FIGURE 2 ENVIRONMENTAL ENVELOPES FOR MAIN STEAM LINE BREAK WITH LOCAL AIR COOLERS AVAILABLE

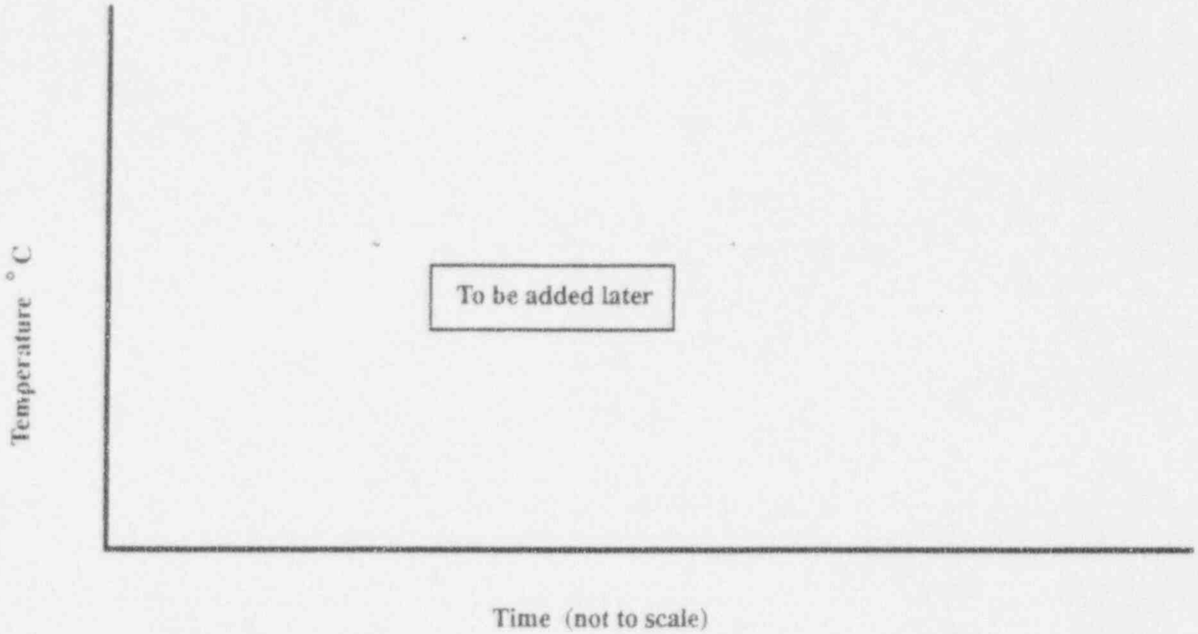


TEMPERATURE ENVELOPE

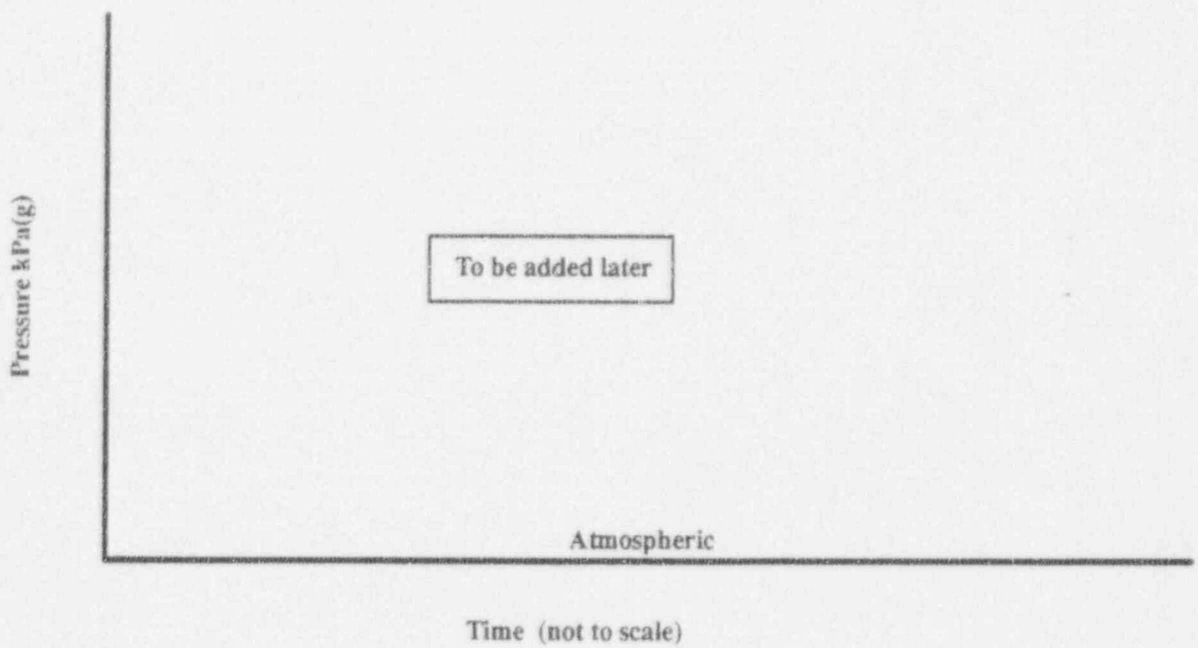


PRESSURE ENVELOPE

FIGURE 3 ENVIRONMENTAL ENVELOPES FOR MAIN STEAM LINE BREAK WITH LOSS OF LOCAL AIR COOLERS



TEMPERATURE ENVELOPE



PRESSURE ENVELOPE

FIGURE 4 ENVIRONMENTAL ENVELOPES FOR SMALL LOCA

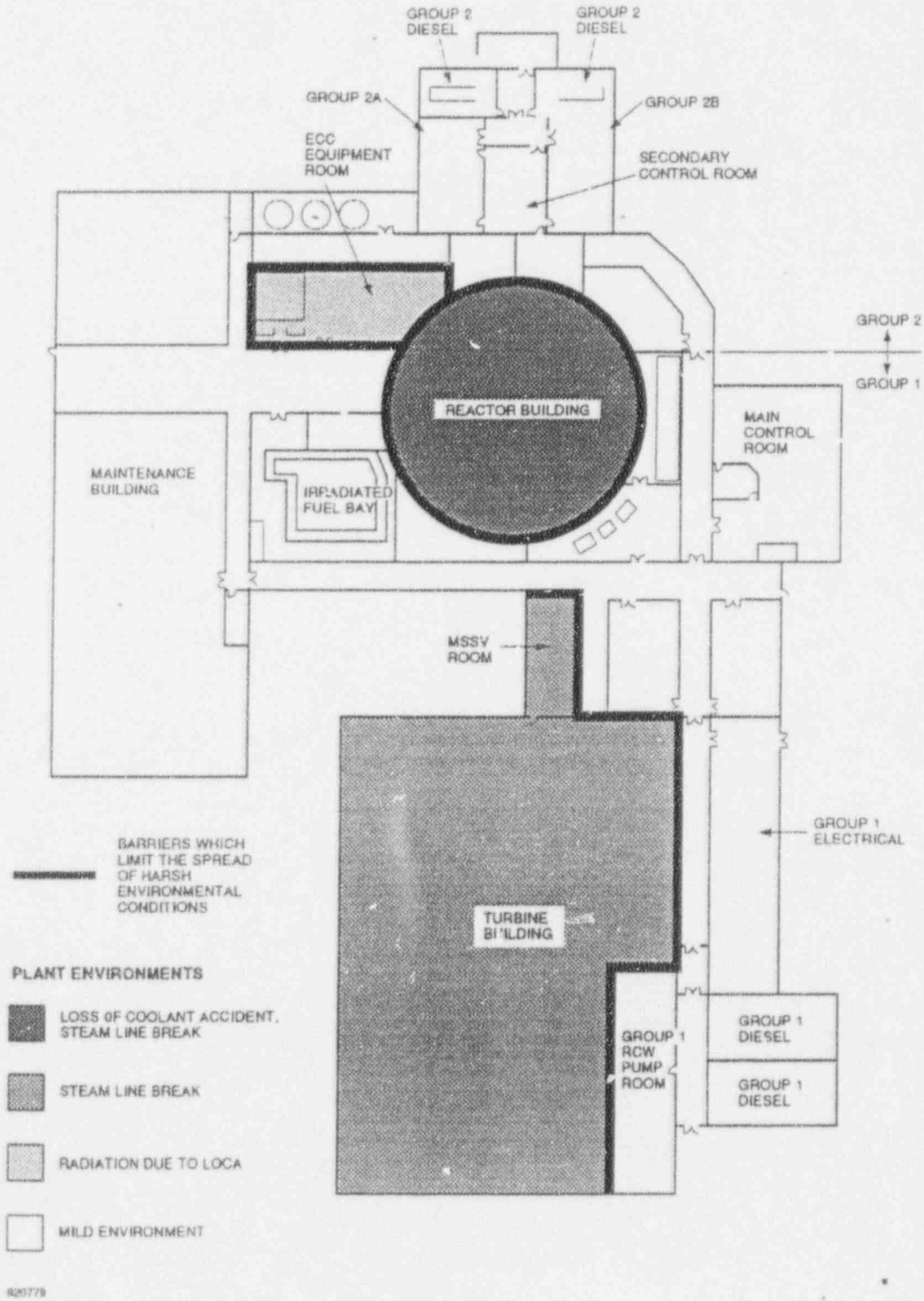


FIGURE 5 PLANT AREAS SUBJECT TO HARSH ENVIRONMENT

APPENDIX A:

LIST OF SAFETY DESIGN GUIDES

Identification	Title
SDG-74-03650-001	Safety Related Systems
SDG-74-03650-002	Seismic Requirements
SDG-74-03650-003	Environmental Qualification
SDG-74-03650-004	Grouping and Separation
SDG-74-03650-005	Fire Protection
SDG-74-03650-006	Code Classification
SDG-74-03650-007	Periodic Inspection
SDG-74-03650-008	Radiation Protection
SDG-74-03650-009	Tornado Protection
SDG-74-03650-010	Pipe Rupture Protection
SDG-74-03650-011	Decommissioning
SDG-74-03650-012	External Flooding