AECL EACL

Safety Design Guide

ENVIRONMENTAL QUALIFICATION

ACR

108-03650-SDG-003

Revision 3

Prepared by
Rédigé par

Nam Seung Deog

Reviewed by
Vérifié par

Johal Hardev S.

Approved by
Approuvé par

Jaitly Raj

Bonechi Massimo

2004/03/16
Controlled

2004/03/16
Contrôlé

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

2251 rue Speakman
Mississauga (Ontario)
Canada L5K 1B2

AECL EACL

Safety Design Guide

Environmental Qualification

ACR

108-03650-SDG-003
Revision 3

2004 March

CONTROLLED

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

Mars 2004

CONTRÔLÉ

2251, rue Speakman
Mississauga (Ontario)
Canada L5K 1B2

AECL EACL

Release and Revision History / Liste des documents et des révisions

0939B Rev. 13

Document Details / Détails sur le document

Title Titre	Total no. of pages N^bre total de pages
Environmental Qualification	39

CONTROLLED - CONTRÔLÉ

Release and Revision History / Liste des documents et des révisions

Release Document No./N°	Release Document Date	Revision Révision No./N°	Revision Date	Purpose of Release; Details of Rev./Amendement Objet du document; détails des rév. ou des modif.	Prepared by Rédigé par	Reviewed by Examiné par	Approved by Approuvé par
1		D1	00-10-13	Issue for 'Review and Comment'	A. H. Stretch K. Reid	A. L. Wight	
2	00-11-23	0	00-11-22	Issued as 'Approved for Use'	A. H. Stretch K. Reid	A.L. Wight	J. Hopwood
3		1D1	02-03-28	Issued for 'Review and Comment'	J.C. Lim	A. H. Stretch	M. Bonechi
4	02-09-11	1D2	02-09-11	Issued for "Review and Comment" Incoporating the latest ACR design changes (e.g., eliminating the "Group"concept, updating ASI, etc)	C. Nie	V. Snell W. Rabbani A. Stretch K. Hau E. Choy A. Josefowicz J. Millard M. Elgohary R. Ghai/O. Hines H. Shapiro H. Johal	

DCS/RMS Input / Données SCD ou SGD

Rel. Proj. Proj. conn.	Project Projet	SI	Section	Serial Série	Sheet Feuille No. N°	Of De	Unit No.(s) Tranche n°
	108	03650	SDG	003	1	4	

AECL EACL

Release and Revision History / Liste des documents et des révisions

0939B Rev. 13

Document Details / Détails sur le document

Title Titre	Total no. of pages Nbre total de pages
Environmental Qualification	39

CONTROLLED - CONTRÔLÉ

Release and Revision History / Liste des documents et des révisions

Release Document No./N°	Release Document Date	Revision Révision No./N°	Revision Date	Purpose of Release; Details of Rev./Amendement Objet du document; détails des rév. ou des modif.	Prepared by Rédigé par	Reviewed by Examiné par	Approved by Approuvé par
5		1	02-10-15	Issued as "Approved for Use".	C. Nie	V. Snell W. Rabbani A. Stretch K. Hau E. Choy A. Josefowicz J. Millard M. Elgohary R. Ghai/O. Hines H. Shapiro H. Johal	M. Bonechi
6		2	03-01-06	Issued as "Approved for Use". Revised as per resolution of comments from the Technical Review. Additions were made to wording of various sections which were mostly of a clarification nature.	C. Nie	J. Tong J. Waddington N. Barkman V. Langman P. Lee H. Johal	M. Bonechi

DCS/RMS Input / Données SCD ou SGD

Rel. Proj. Proj. conn.	Project Projet	SI	Section	Serial Série	Sheet Feuille No. N°	Of De	Unit No.(s) Tranche n°
	108	03650	SDG	003	2	4	

AECL EACL

Release and Revision History / Liste des documents et des révisions

0939B Rev. 13

Document Details / Détails sur le document

Title Titre	Total no. of pages Nbre total de pages
Environmental Qualification	39

CONTROLLED - CONTRÔLÉ

Release and Revision History / Liste des documents et des révisions

Release Document No./N°	Release Document Date	Revision Révision No./N°	Revision Date	Purpose of Release; Details of Rev./Amendement Objet du document; détails des rév. ou des modif.	Prepared by Rédigé par	Reviewed by Examiné par	Approved by Approuvé par
7		3	04-03-16	Issued as "Approved for Use". Major changes are due to impact of safety design guide supplement (SGS-002: "Safety Basis impact on EQ"). Minor text additions are identified by underlining and major text additions and deletions are noted in this revision history. Revisions consist of the following: • Section 3: removed the reference of CSA Standard N290.13 (Draft) • Section 3.2 c): removed reference to the failure of SG blowdown system and Post LOCA instrument air system • Section 3.3: added second and third paragraphs to introduce safety analysis basis EQ approach - revised i) LOCA in subsection b) - added new text for event cases: b) 1) ii)LOCA+LOCLIV, b) 1) iv) other limited core damage accidents, b) 3) In-core LOCA • Added new Section 3.5 "Temperature and Pressure Profiles for EQ of Equipment" • Section 6: added references [8] and [9] • Table 1: revised table to clarify applicable bounding event and added note ##	S.D. Nam	H. Johal	R. Jaitly / M. Bonechi

DCS/RMS Input / Données SCD ou SGD

Rel. Proj. Proj. conn.	Project Projet	SI	Section	Serial Série	Sheet Feuille No. N°	Of De	Unit No.(s) Tranche n°
	108	03650	SDG	003	3	4	

AECL EACL

Release and Revision History / Liste des documents et des révisions

0939B Rev. 13

Document Details / Détails sur le document

Title / Titre	Total no. of pages / N^bre total de pages
Environmental Qualification	39

CONTROLLED - CONTRÔLÉ

Release and Revision History / Liste des documents et des révisions

Release Document No./N°	Date	Revision Révision No./N°	Date	Purpose of Release; Details of Rev./Amendement / Objet du document; détails des rév. ou des modif.	Prepared by / Rédigé par	Reviewed by / Examiné par	Approved by / Approuvé par
				- Replaced ASI number 32200 by 32210 - Removed "Feed Pumps" in ASI 33310 - Removed "MSLB" applicable bounding event for feedwater system in ASI 43230 - Added ASI 66100 Main Control Room - Replaced ASI number 68631 by 67312 - Added "##" note in the column of systems and major components of ASI numbers 32100, 34110, 34340, 68480 and 73110 • Figures 1 and 2: removed to be added after analysis is available • Figure 3: updated plant layout design • Acronym table updated more specific to ACR			

DCS/RMS Input / Données SCD ou SGD

Rel. Proj. / Proj. conn.	Project / Projet	SI	Section	Serial / Série	Sheet / Feuille No. / N°	Of / De	Unit No.(s) / Tranche n°
	108	03650	SDG	003	4	4	

TABLE OF CONTENTS

SECTION **PAGE**

TABLES

FIGURES

TABLE OF CONTENTS

SECTION **PAGE**

APPENDICES

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, and the requirements to be addressed by designers 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 0729-00.

3. ENVIRONMENTAL QUALIFICATION PHILOSOPHY

This section of the Safety Design Guide describes the safety concept and the safety design philosophy used to develop the safety requirements for environmental qualification. It is to be considered as information for the interpretation and application of the safety requirements in Section 4.

Further guidance on environmental qualification is provided in the IAEA Nuclear Safety Design Guide Standards Series No. NS-R-1 [Reference 1] and IEEE 323 [Reference 6].

3.1 Environmental Qualification Program

Safety related systems and components that are required to perform safety functions during accident conditions must be designed to withstand the environmental conditions that occur as a consequence of the accident. Where these conditions are severe, and the equipment operability can potentially be affected by its 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. Structures are designed to withstand the harsh conditions to the extent that the required safety functions can be performed, and are not included in the Environmental Qualification Program.

Equipment credited in the safety analysis with performing a function following a design basis event must be environmentally qualified to ensure that it will function as required, during and following any environmental transient resulting from the event.

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) Design basis 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, that 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 analysed 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, because the conditions are similar to those during normal plant operation. Environmental qualification is not required for these conditions, although analysis or tests may be done as part of the normal design process for specific equipment to show that the equipment can perform its function during normal operation of the plant.

Harsh environmental conditions exceed normal operating conditions, including elevated temperature, pressure, humidity, and radiation levels, and result from accident conditions. Events such as loss of coolant accidents and steam line failures (steam line failures include feedwater line failures) produce the bounding environmental conditions. The harsh pressure and temperature conditions shown in Figures 1 and 2 (to be completed after analysis is available) are recommended as an upper bound envelope for the plant. The harsh radiation condition shall be based on the Radiation Dose Rates analysis results for Environmental Qualification document. For these conditions, qualification is necessary to demonstrate that the required safety function can be reliably performed.

The areas of the plant affected by the harsh environment are restricted to the specific areas shown in Figure 3, which are:

a) Reactor Building

   Systems and components in this area will be subject to harsh pressure and temperature conditions and to the harsh radiation condition. Flooding can occur in the bottom of the building, and the potential flood level must be calculated for Loss of Coolant Accident (LOCA), and other events which would cause flooding. Equipment must be located above the flood level for events which the equipment is required to mitigate, or be shown to be operable in a submerged condition.

b) Reactor Auxiliary Building – Long-Term Cooling (LTC) 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. (The LTC piping within the room is part of the containment boundary, but the room is not.)

c) Reactor Auxiliary Building

   Systems and components in this area will be subject to a mild environment. Piping connected to the reactor building ventilation system is designed to remain intact in the event of a LOCA and loss of containment isolation. This piping shall be located to avoid exposing areas containing non-environmentally qualified safety related equipment or plant staff to high radiation fields.

d) Main Steam Safety Valve (MSSV) / Main Steam Isolation Valve (MSIV) Room

The MSSVs and MSIVs and their associated power supplies and instrumentation will be subject to saturated steam due to a pressure boundary failure in the room (e.g., piping, valve), with very little radiation.

e) Turbine Building

Systems and components in this area will be subject to a saturated steam atmosphere at low pressure with very little radiation. The valves interconnecting the steam lines in this area may be safety related, 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 that perform essential safety functions during events causing harsh environmental conditions are described below. Components of these systems are either protected from the harsh environment, or qualified to withstand it[1].

The document "Safety Basis for ACR" [8] on the safety analysis approach proposes five classes of events to meet the intent of CNSC Consultative Document C-006 (Rev. 1) [9]. Design basis events include the Class 1 to Class 3 events, whereas the Limited Core Damage Accidents (LCDAs) are Class 4 and Class 5 events.

As per the Safety Basis [8] approach, environmental conditions for ACR will be based on design basis events along with the assumption of the Single Failure Criterion (SFC). The systems and equipment credited to function for design basis events will be qualified to operate for the harsh conditions from the design basis events. While the systems and components required to perform safety functions during and after the LCDAs will not be part of the formal environmental qualification program, such equipment will be assessed on case-by-case basis to provide reasonable assurance of their capability to operate via design assessments or Probabilistic Safety Assessment (PSA).

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 that must withstand these events are also included in Table 1 and indicated conceptually in Figure 3.

---

1 It may not always be necessary to qualify the entire system. Only the equipment where response is necessary to ensure the system safety function is adequately performed, needs to be qualified.

a) Shutdown:

The reactor will be shut down by either SDS1 or SDS2, so components of both systems that 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 shutdown 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.

b) Fuel Cooling:

The systems and equipment that provide fuel cooling for different events are qualified as follows:

1) Large LOCA

Large LOCA is a design basis event. The initiating event is a large break in a Heat Transport System (HTS) header pipe. The heat transport system is designed so that overheating of the fuel is prevented until such time that reactor shutdown is achieved and long term fuel cooling is established to remove decay heat.

i) LOCA

The Emergency Core Cooling (ECC) system, consisting of two sub-systems, Emergency Coolant Injection (ECI) system and Long Term Cooling (LTC) system, is qualified to cool the fuel. The support services needed for operation of these systems are qualified to remain available (i.e., feedwater, electrical power, and cooling water). The fuelling machine is qualified to remain on-reactor (i.e., remains connected and motionless).

ii) LOCA + LOCLIV

Large LOCA with loss of Class IV power is a design basis event. There is a small possibility that this disruption to the grid will result in a loss of off site power. When Class IV power is lost, the standby diesel generators are signalled to start. A LOCA signal occurs on the ECI initiation signal conditioned on reactor building high-pressure. This occurs before the LOCA signal, which would also signal the standby diesel generators to start. The isolation valves in the reserve water system open to allow water to flow from the reserve water tank to the sump. The fuel cooling will be provided by the steam generators, and two of the Long Term Cooling pumps are started in recirculation mode.

iii) LOCA + LOECC

Large LOCA with loss of ECC is a limited core damage accident. For this event, the emergency core cooling system is unavailable, and the moderator system provides fuel cooling. The electrical system and recirculated cooling water system that provide services to the moderator system are qualified to remain available. The shield cooling system is designed to maintain its inventory for long term cooling. The moderator cover gas system is designed to ensure an adequate moderator subcooling temperature by maintaining pressure on the moderator in the calandria.

The Reserve Water System (RWS) can provide water to the heat transport system as a short-term heat sink for this event. The hydrogen control system is available to control the presence of the hydrogen produced during this event.

iv) Other Limited Core Damage Accidents

Limited core damage accidents including the above iii) are extremely low frequency events, which must be accommodated within specified radiological dose limits to the public. Most LCDAs are combinations of an initiating event and the total failure or failure of subset of a safety system.

2) Small LOCA

Small LOCA is a design basis event. For purposes of environmental qualification, a small LOCA is considered to be a break which exceeds the makeup capability of the heat transport H_2O feed pumps. Breaks smaller than this size are considered to be leaks, and will cause only local effects, and will not result in harsh environmental conditions affecting other mitigating systems (also see 6) below).

The small LOCA events include fuel channel feeder breaks and smaller breaks for which the HTS does not depressurise fast enough to introduce the ECI cooling water into the HTS due to the small break size. The fuel cooling will be provided by the steam generators, so the associated feedwater systems and associated level controls will be qualified for this event. 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 (e.g., the HT liquid relief valves, etc.).

3) In-core LOCA

The initiating event is assumed to be a pressure tube and calandria tube rupture (Class 3 event). For in-core LOCA, the event sequence in containment is different from the small LOCA in a reactor header, because the discharge is into the moderator rather than directly to containment. The coolant discharge is initially absorbed and cooled by the moderator unless it is at a high location in the core. During or after the reactor trips on one of the process-trips on either or both of the two shutdown systems, the fuel cooling is provided by the steam generators, so the associated feedwater systems and associated level controls must remain available for this event. After the LOCA signal initiation, decay heat removal process will be similar to a small LOCA.

4) Main Steam Line Breaks (MSLB) inside Reactor Building

A main steam line break in reactor building is a design basis event. 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 support systems (auxiliary feedwater, electrical power) are qualified to maintain feedwater flow to the steam generators. The reserve water system is also qualified to provide a back-up water supply 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 automatically or manually. The makeup for HTS shrinkage will be provided by the qualified emergency coolant injection system. The heat is rejected through the breaks and MSSVs, 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.

5) Main Steam Line Breaks outside Reactor Building

A main steam line break outside reactor building is a design basis event. 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 "4)" above. In this case, the MSSVs and MSIVs and their services in the MSSV/MSIVs room will be qualified for the environment resulting from a piping failure in that area. For main feedwater line breaks, the auxiliary feedwater system or the reserve water system supply (make-up water) is provided to the steam generators. The wall between the turbine building and crane hall prevents the harsh environment from extending beyond the turbine building.

6) Other

Heat transport system leaks, up to the capacity of the H_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 evaluated during design, to ensure that sufficient equipment remains available to perform the essential safety functions.

c) Containment:

The containment boundary will be maintained for events during which a release may occur, to satisfy the requirement of CNSC Regulatory Document R-7. The containment penetrations, local air coolers, containment isolation components, hydrogen control components, and post-accident monitoring components are qualified or located in areas not subject to the harsh environment. For steam generator tube failures, the containment boundary will be formed by closure of MSIVs.

In general, all internal structures must be able to withstand the maximum differential pressure in containment.

d) Monitoring and Control:

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

3.4 Environmental Qualification Design Principles

The design of the plant incorporates the following principles to minimize the number of safety related components that 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 LTC room in 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. Systems that contain high energy, such as steam lines and feedwater lines, are routed outside of the reactor auxiliary building (RAB) or along protected routes to avoid harsh environmental conditions in the RAB or areas containing safety related equipment.

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, or above, areas subject to flooding.

e) Safety related components are standardized to reduce the amount of environmental qualification (i.e., components located in a similar or comparable type of environment, but less severe as the environmentally qualified component shall also be considered environmentally qualified).

3.5 Temperature and Pressure Profiles for Environmental Qualification of Equipment

As high energy piping systems are kept out of the Reactor Auxiliary Building (RAB) and equipment located in the Turbine Building (TB) is not credited for any high energy pipe break in the TB, the temperature and pressure profiles are mainly required for the Reactor Building (RB). Harsh environmental conditions caused by a LOCA and steam line break in the RB are quite different, and therefore, profiles for a LOCA and steam line break are presented in Figures 1 and 2 (to be completed after analysis is available).

It is designers' decision to choose the appropriate profiles depending on the accident for which a system is required to be operable. Steam line break conditions presented for the RB, bound the feedwater line break conditions.

LOCA and steam line break conditions are taken from the safety analysis cases; safety analysis is carried out for these events with the assumption of a limiting single failure in a mitigating system.

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.

b) The EQ program documents shall contain sufficient information to ensure that the qualification of required components can be maintained during construction and operation of the plant.

c) The plant design shall consider all events that could cause harsh environmental conditions.

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

e) The barriers shown in Figure 3 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 minimized. Where they are necessary, they shall be designed to avoid propagation of the harsh environmental conditions to areas of mild environment that contain essential safety related components. Additional barriers shall be provided, where necessary, to protect specific components from localized effects of events, consistent with the separation concepts included in 108-03650-SDG-004 [Reference 4]. The structural design of these barriers may use pressure and temperature conditions derived directly from the analysis of the relevant events, with an appropriate margin, rather than the upper bound conditions recommended in this safety design guide.

f) Steam lines, feedwater lines and steam generator blowdown lines that are connected to the steam generators and which contain high energy shall have provision to protect the reactor auxiliary building from the failure of those lines.

g) The designer shall calculate the flood level in the reactor building for the event(s) causing the largest fluid release, and shall ensure that equipment which performs a safety function during an event causing flooding is located above the design flood level. The designer shall also investigate the "rivulet" effects from water flowing down vertical surfaces to ensure the safety related equipment is properly protected.

h) All internal structures shall be able to withstand the maximum differential pressure in containment.

i) The environmental conditions created by an accident (LOCA or steam line break) shall be appropriately considered by designers for any impact on stress analysis of piping systems and components.

j) Paint used for equipment inside the reactor building shall be qualified to the LOCA condition to ensure that paint will not peel or delaminate during a LOCA event.

k) Installation instruction/procedures shall clearly identify installation requirements for maintaining environmental qualification configuration in the field.

4.2 Components to be Qualified

a) For each event creating harsh environmental conditions, the safety related systems required to perform the safety functions of reactor shutdown, heat removal from the core, containment, plant control and monitoring, and support services shall be identified. (See 108-03650-SDG-001 [Reference 5] 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, environmentally qualified, or assessed as being able to withstand the conditions without further qualification.

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 analysed, 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 that result from accident conditions caused by events such as a loss of coolant accident or a steam line break (including feedwater line break and steam generator blowdown line break).

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),
   6) water flowing down vertical surfaces.

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. In particular, the effects of any chemicals added to the ECC water during a LOCA or other chemicals that may have been added to the source of water that is giving rise to the harsh environment shall be evaluated.

d) The curves in Figure 1 and Figure 2 (to be completed after analysis is available) envelope the recommended upper bound temperature and pressure transients predicted 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.[2]

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. Where temperature and pressure curves cannot be matched exactly, the temperature curve shall be followed to produce a saturated steam condition.

h) The radiation doses used for qualification of components shall be derived from 108-03320-AR-001 "Radiation Dose Rates for Environmental Qualification", 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, 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, humidity, water

---

2 If the structure or component does not pass the qualification test, the designer can select to qualify them for individual accident profiles.

spray and flooding. 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. Those that can be shown to withstand the harsh conditions by engineering assessment (e.g., metal components) may be qualified by engineering assessment rather than formal test.

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 be 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. Where it is necessary to supply non-qualified equipment from a qualified power supply then the requirements of IEEE 308 shall be followed;

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

c) Guidance for acceptable qualification methods for electrical components is given in IEEE-323 "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" [Reference 6]. In applying the IEEE standard, it should be noted that references to seismic events are not applicable, and that Safety Design Guide 108-03650-SDG-002 [Reference 2] shall be used instead, as Canadian regulatory requirements do not require consideration of a simultaneous earthquake and LOCA. In addition, IEC 60780 "Nuclear Power Plants – Electrical Equipment of the Safety System – Qualification" [Reference 7] should be consulted.

d) Type tests are the preferred method of qualification; where type tests are impractical, justification documented by 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 mission period for systems and components shall be based on the length of time required to successfully mitigate the consequences of a bounding design basis accident.

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 and IEC 60780. 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 margins should not be overly conservative.

h) Many non-metallic materials, particularly polymers, display aging mechanisms that may affect their safety 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 could affect the safety function of a component, 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 well documented operating experience.

i) 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.

j) 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

a) A layout review (site walkdown) shall be done during the late stages of construction/commissioning to confirm that the location and installation of the environmentally qualified equipment conforms to the location as analysed in the environmental qualification documents. Such a review shall be performed on two systems to confirm that the environmentally qualified components have been installed properly; results of this review shall be used to determine if a full scale layout review of all environmentally qualified components is necessary. Field run equipment that is environmentally qualified should be installed according to specific procedures to maintain that qualification and should be checked after installation for potential local effects during the layout review.

b) 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.

5. DOCUMENTATION

a) The design documentation shall identify the environmentally qualified systems, the performance required, preferably in measurable term, the safety functions performed, the events for which the safety function is needed, the environmentally qualified components in each system, and their mission time.

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 (including drawings), to be recorded in a database, 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 more severe or less severe 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 and functional 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) any maintenance requirements to maintain the qualification in operation (e.g., for seal or local barriers);
   14) 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:
   i) a description of the test facility and instrumentation with calibration traceability records;
   ii) the test procedure;
   iii) the test data and accuracy;
   iv) the test failures and any other pertinent information, and their resolution satisfactory to both the supplier and AECL.

f) The supplier/laboratory shall identify 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, measures, such as equipment redesign by the supplier, shall be taken to eliminate such failures in the future, and the equipment retested.

g) Based on the above documents, an EQ database is recommended to be set up for ease of reference.

6. REFERENCES

[1] IAEA, "Safety of Nuclear Power Plants": Design, Safety Standards Series No. NS-R-1, IAEA, Vienna.

[2] Safety Design Guide 108-03650-SDG-002 "Seismic Requirements".

[3] Safety Design Guide 108-03650-SDG-006 "Containment".

[4] Safety Design Guide 108-03650-SDG-004 "Separation of Systems and Components".

[5] Safety Design Guide 108-03650-SDG-001 "Safety Related Systems".

[6] IEEE Std 323-2003, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations".

[7] IEC 60780, "Nuclear Power Plants – Electrical Equipment of the Safety System – Qualification", Second Edition 1998-10.

[8] Analysis Basis Document, 108-03600-AB-003 "Safety Basis for ACR", Rev. 0, 2003-09.

[9] CNSC Draft Regulatory Guide C-006, "Safety Analysis of CANDU Nuclear Power Plant", Rev. 1 (E), 1999-09.

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

ASI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event (Figure 1 and Figure 2)
20000	Buildings and Structures		
21000	Reactor Building	To maintain an effective barrier to release of radioactive material to the outside of the building.	LOCA
		To maintain structural integrity and prevent propagation of harsh environment to other areas of the plant.	MSLB
21600	Special Equipment (airlocks, shielding doors, blowout panels, etc.)	To maintain an effective barrier to release of radioactive materials to the outside of the building.	LOCA MSLB
		To prevent propagation of harsh environment to other areas of the plant.	LOCA MSLB
22000	Turbine Building	To prevent propagation of harsh environment to other areas of the plant.	MSLB#
24000	Reactor Auxiliary Building (LTC Room)	To prevent propagation of high radiation environment to other area of the building.	LOCA
24xxx	MSSV/MSIV Room	To prevent propagation of harsh environment to other areas of the plant.	MSLB#
30000	Reactor, Reactor Systems and Auxiliary System		
31000	Reactor (also see ASI 32100 and 33100)	To maintain integrity of HTS and provide support for reactor control mechanisms and other interfacing fuel cooling systems.	See below
31700	Reactivity Control Units		
31730	Shutoff Units	To provide reactor shutdown. (See ASI 68200)	LOCA MSLB

ASI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event (Figure 1 and Figure 2)
31740	In-Core Flux Detector Units	To provide signals for reactor shutdown. (See ASI 68200, 68300)	LOCA MSLB
31760	Liquid Injection Shutdown Units	To provide reactor shutdown (See ASI 68300)	LOCA MSLB
31790	Ion Chamber Units	To provide signals for reactor shutdown.	LOCA MSLB
32000	Moderator and Auxiliary Systems		
32100	Moderator System ##	To remove heat from the fuel for a LOCA with loss of ECC.	LOCA
		To maintain integrity so as not to drain moderator.	LOCA
32210	Moderator Purification System Isolation valves	To be able to isolate the moderator system to prevent inadvertent poison removal.	LOCA MSLB
32300	Moderator Cover Gas System	To ensure adequate moderator subcooling.	LOCA
		To prevent radioactive release.	MSLB
32700	Moderator Liquid Poison System	To add poison to moderator.	LOCA MSLB
33000	Heat Transport and Auxiliary Systems		
33100	Heat Transport - heat transport system pressure boundary and isolation valves.	To maintain inventory of heat transport coolant.	MSLB LOCA
33120	Heat Transport System equipment – pumps	To provide forced circulation of HTS coolant if necessary (to be confirmed by analysis).	LOCA
33310	Heat Transport Pressure and Inventory Control System		
	Pressurizer	To accommodate coolant volume change in the HTS.	MSLB LOCA
	Liquid Relief Valves	To maintain the HTS pressure boundary and provide over pressure protection for the HTS.	MSLB LOCA
	Pressurizer Steam Relief Valves	As above	MSLB LOCA

ASI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event (Figure 1 and Figure 2)
33340	Heat Transport Pump Seal System	To provide cooling, if required, to HTS pump seals so as to maintain seal integrity.	LOCA MSLB
34000	Auxiliary Systems		
34110	Shield Cooling System ##	To ensure calandria vessel integrity for a LOCA and LCDAs; make up to this system is also provided for severe core damage scenarios.	LOCA
34320	Emergency Coolant Injection System	To provide injection of coolant to the HTS.	LOCA
		To provide makeup for HTS shrinkage.	MSLB
34340	Reserve Water System ##	To provide a water supply and/or heat sink capability to the shield tank, HTS, moderator system, S/G, and LTC system.	LOCA MSLB
34350	Long-Term Cooling System*	To remove decay heat from the HTS following reactor shutdown and provide long-term coolant recirculation and heat removal to the HTS following a loss coolant accident.	MSLB LOCA
34710	Liquid Injection Shutdown System (see ASI 68300)	To provide reactor shutdown.	LOCA MSLB
35000	Fuel Handling and Storage		
35100	New Fuel Transfer and Storage	To maintain the containment boundary.	LOCA MSLB
		Not breach containment when the F/M is near the New Fuel Port.	
35200 35730	Fuel Changing- (Fuelling Machine Head, Catenary, Carriage, Bridge) (FM) Cable and Hose Management System	To maintain the 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).	MSLB LOCA

ASI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event (Figure 1 and Figure 2)
		Not to overstress the end-fitting when the F/M head is on reactor face.	
		Not breach the pressure boundary integrity of HTS when the F/M is near the reactor face.	
		To cool the fuel enough to prevent failures when spent fuel is in the F/M and the F/M is off-reactor (that is, in transit).	
35300	Spent Fuel Transfer and Storage	To maintain the containment boundary.	LOCA MSLB
		To prevent drainage of the spent fuel bay water into the reactor building.	
		Not breach containment when the F/M is near the Spent Fuel Port.	
		To maintain fuel cooling when spent fuel is in the SF Transfer system to prevent spent fuel failures.	
36000	Steam Generator Systems		
36100	Steam and Relief Systems (Main Steam Safety Valves/Main Steam Isolation Valves*)	To remove heat from the steam generators following reactor shutdown, and isolate steam generators following MSLB.	MSLB# LOCA (including Steam Generator Tube Rupture (SGTR))
36310	Steam Generator Blowdown System	To be able to isolate the steam generator from the break to maintain the capability of the steam generator to remove heat from the HTS.	LOCA MSLB (S/G blowdown system pipe break)
43000	Feedwater and Auxiliary Steam Systems		

ASI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event (Figure 1 and Figure 2)
43230	Feedwater System	To provide feedwater and control to the steam generators.	Small LOCA
	Feedwater check valve inside the R/B	To prevent outflow of water from the secondary side of the steam generator.	MSLB
50000	Electric Power Systems		
51000	Cables and Connections Class III Power	To provide power for mitigating system (moderator) operation when Class IV power is unavailable.	LOCA MSLB
	Cables and Connections Class II Power	To provide uninterruptible AC power to mitigating systems.	LOCA MSLB
	Cables and Connections Class I Power	To provide uninterruptible DC power to mitigating systems.	LOCA MSLB
53000	Distribution System	As above	As above
57000	Cabling System	To provide an electrical power supply to mitigating systems/components which are located in harsh environment and needed for events.	LOCA MSLB
57600	Containment Penetrations	To maintain an effective barrier to the release of radioactive materials.	LOCA
		To prevent propagation of harsh environment to other areas of the plant.	MSLB
60000	Instrumentation and Control		
	The applicable I&C systems mentioned in this table, for equipment in a harsh environment.	To provide signals for control and monitoring of 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 applicable ASI
66000	Control Centre		

ASI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event (Figure 1 and Figure 2)
66100	Main Control Room**	To provide control and monitoring.	LOCA MSLB
66600	Secondary Control Area **	To provide control and monitoring if the control centre becomes unavailable.	LOCA MSLB
67312	Reactor Building Ventilation System	To close isolation dampers on the ventilation ducts to minimize release of radioactive material.	LOCA
67314	Containment Isolation	To maintain an effective barrier to release of radioactive materials to the outside of the building.	LOCA
		To prevent propagation of harsh environment to other areas of the plant.	MSLB
68000	Safety Systems		
68200	Shutdown System No. 1 (SDS1)	To provide signals for reactor trip and maintain it in a safe shutdown.	LOCA MSLB
68300	Shutdown System No. 2 (SDS2)	To provide signals for reactor trip and maintain it in a safe shutdown.	LOCA MSLB
68400	Containment System (see ASI 67314 for Containment Isolation System)	To provide signals for actuation of containment system.	LOCA MSLB
68480	Hydrogen Control System ##	To provide control of H_2/D_2.	LOCA
68570	Second Crash Cooldown System	To open some MSSVs to ensure heat transport system depressurization	LOCA
68900	Post Accident Management	To provide monitoring of safety related systems after an event.	Refer to ASI for individual systems
70000	Common Processes and Services		
71000	Water Systems		
71300 71310 71340	Service Water Systems Raw Service Water System * Recirculated Cooling Water System*	To remove decay heat, after reactor shutdown and initial cooldown, from the shutdown cooling system. To remove heat from the moderator system, after LOCA+LOECC.	LOCA MSLB#

ASI	Systems and Major Components	Safety Functions to be Performed by Qualified Systems	Applicable Bounding Event (Figure 1 and Figure 2)
73000	Heating, Cooling and Ventilation Systems		
73110	Containment Cooling System ##	To reduce containment temperature and pressure, and to provide hydrogen mixing after a LOCA.	LOCA MSLB
73120	Reactor Building Ventilation System	To prevent propagation of harsh environment to other areas of the plant.	MSLB
73140	Containment Isolation (Also see ASI 68400 and 67314)	To provide containment isolation.	LOCA MSLB
75000	Compressed Gases		
75120	Instrument Air System	To provide back-up instrument air supplies to qualified mitigating systems.	LOCA MSLB

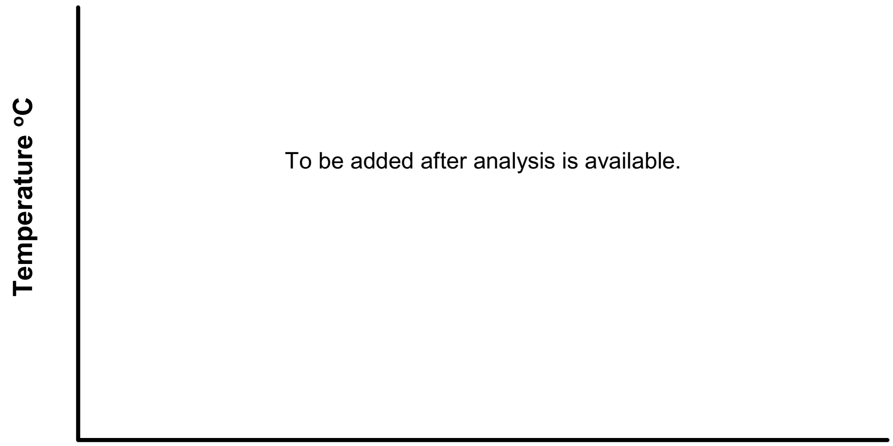
Notes:

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

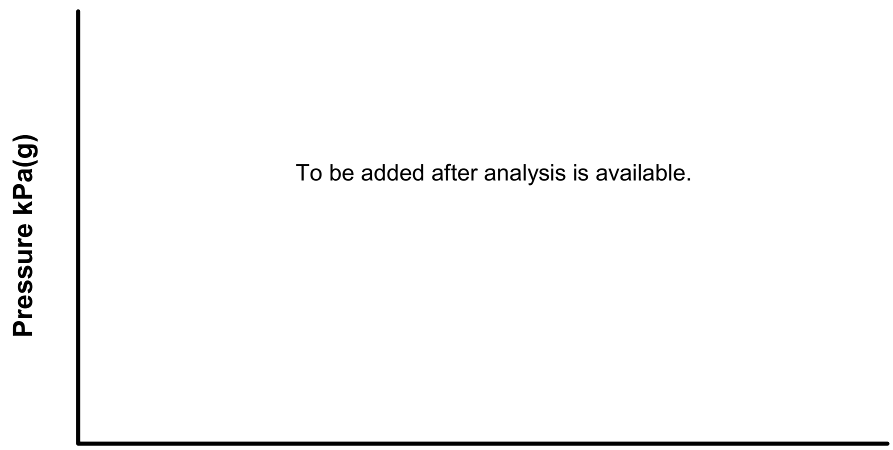
** There are probably no EQ implications here. It is more to indicate the items shall be available for applicable bounding events.

Outside of the reactor building, use specific conditions for that location.

These systems and equipment perform functions for the limited core damage accidents and/or severe core damage accidents.

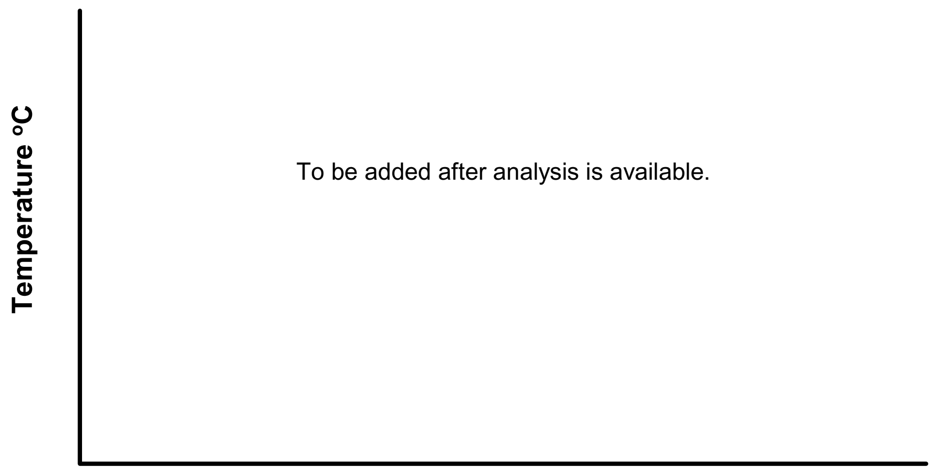


TEMPERATURE ENVELOPE

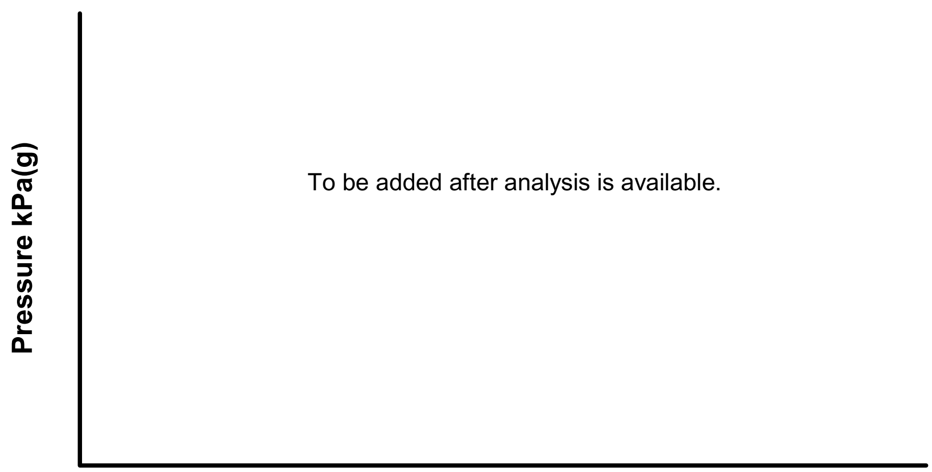


PRESSURE ENVELOPE

Figure 1 Environmental Envelopes for LOCA



TEMPERATURE ENVELOPE



PRESSURE ENVELOPE

Figure 2 Environmental Envelopes for Main Steam Line Break

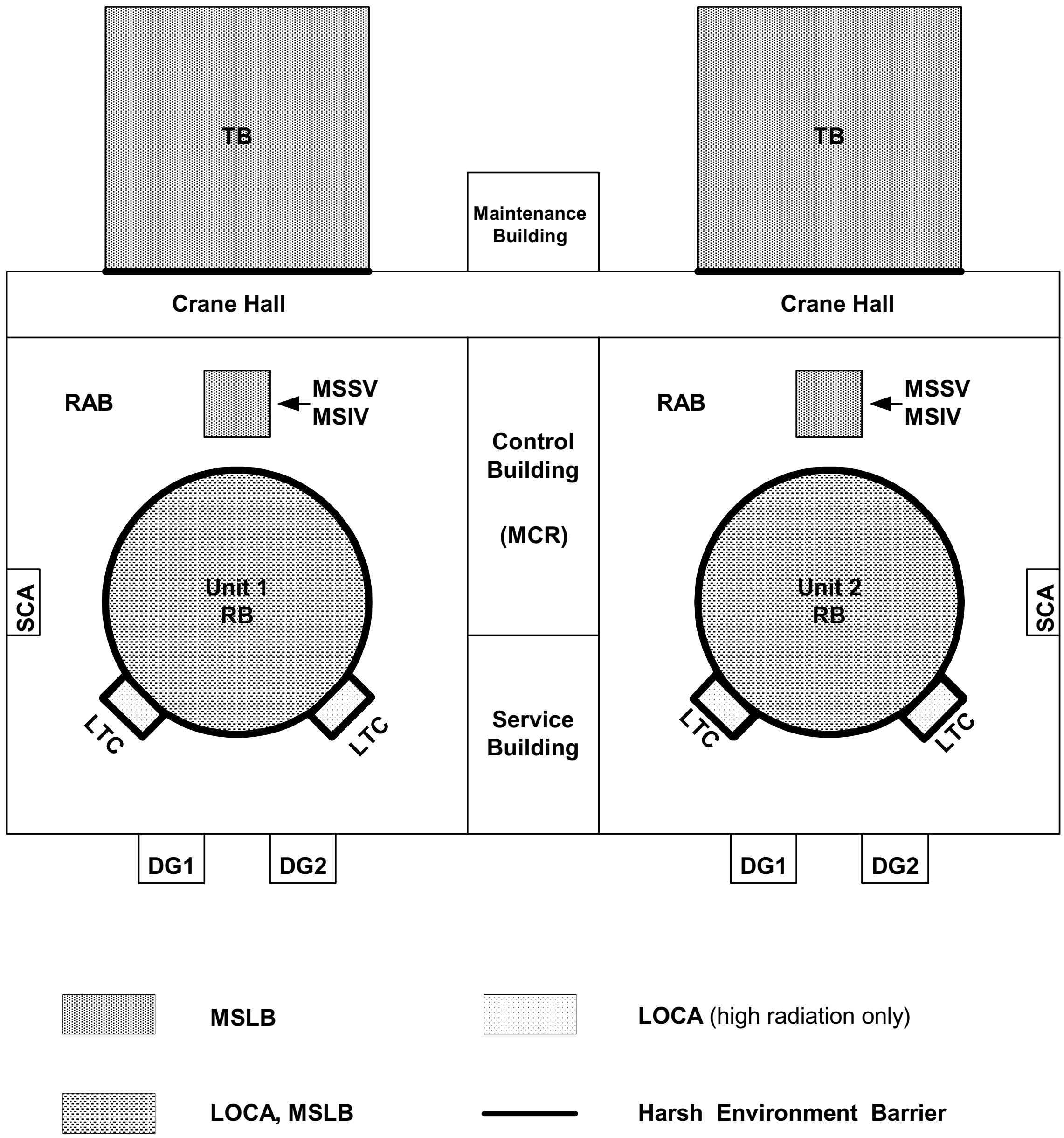


Figure 3 Plant Areas Subject to Harsh Environment (Conceptual Schematic)

Appendix A

List of Safety Design Guides

Identification	Title
108-03650-SDG-001	Safety Related Systems
108-03650-SDG-002	Seismic Qualification
108-03650-SDG-003	Environmental Qualification
108-03650-SDG-004	Separation of Systems and Components
108-03650-SDG-005	Fire Protection
108-03650-SDG-006	Containment
108-03650-SDG-007	Radiation Protection

Appendix B

Acronyms

AC	Alternating Current
ACR™*	Advanced CANDU Reactor™
AECL	Atomic Energy of Canada Limited
ALARA	As Low As Reasonably Achievable
ASDV	Atmospheric Steam Discharge Valves
ASI	AECL Subject Index
BOP	Balance Of Plant
CA	Control Absorber
CANDU®	Canadian Deuterium Uranium
CCP	Critical Channel Power
CCW	Condenser Cooling Water
CHF	Critical Heat Flux
CNSC	Canadian Nuclear Safety Commission
COG	CANDU Owners Group
CSA	The Canadian Standards Association
D_2O	Heavy Water
DBE	Design Basis Earthquake
DC	Direct Current
DCS	Distributed Control System
DEL	Derived Emission Limit
DG	Diesel Generator
EAB	Exclusion Area Boundary
ECCS	Emergency Core Cooling System
ECI	Emergency Core Injection
EDS	Electrical power Distribution System
HTS	Heat Transport System
IAEA	International Atomic Energy Agency
ICRP	International Commission for Radiation Protection
ISO	International Organization for Standardization
LCDA	Limited Core Damage Accident
LOCA	Loss Of Coolant Accident
LTC	Long Term Cooling

* ACR™ (Advanced CANDU Reactor™) is a trademark of Atomic Energy of Canada Limited (AECL).

® CANDU is a registered trademark of Atomic Energy of Canada Limited.

LWR	Light Water Reactor
MCR	Main Control Room
MOT	Main Output Transformer
MSIV	Main Steam Isolation Valves
MSSV	Main Steam Safety Valves
NEW	Nuclear Energy Worker
NSP	Nuclear Steam Plant
NSSS	Nuclear Steam Supply System
OM&A	Operation, Maintenance and Administration
PAM	Post Accident Management
PSA	Probabilistic Safety Assessment
PTR	Pressure Tube Reactor
PWR	Pressurized Water Reactor
RAB	Reactor Auxiliary Building
RB	Reactor Building
RCU	Reactivity Control Unit
RCW	Recirculated Cooling Water
RSW	Raw Service Water
RWS	Reserve Water System
SCA	Secondary Control Area
SDS 1	Shut Down System 1
SDS 2	Shut Down System 2
SEU	Slightly Enriched Uranium
SGTR	Steam Generator Tube Rupture
SFC	Single Failure Criterion
SST	System Service Transformer
SU	Shutoff Unit
ULC	Underwriter's Laboratories Canada
UPS	Uninterrupted Power Supply
UST	Unit Service Transformer
ZCU	Zone Control Unit