AECL EACL

Safety Design Guide

SAFETY RELATED SYSTEMS

ACR

108-03650-SDG-001

Revision 3

Prepared by
Rédigé par

Chan Patrick

Reviewed by
Vérifié par

Johal Hardev S.

Approved by
Approuvé par

Jaitly Raj | Bonechi Massimo

2004/03/26
Controlled

2004/03/26
Contrôlé

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

2251 rue Speakman
Mississauga (Ontario)
Canada L5K 1B2

AECL EACL

Safety Design Guide

Safety Related Systems

ACR

108-03650-SDG-001
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 / Nbre total de pages
Safety Related Systems	65

CONTROLLED - CONTRÔLÉ

Release and Revision History / Liste des documents et des révisions

Release Document No./N°	Release Document Date	Revision Révision No./N°	Revision Révision 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	00-04-05	0D1	00-03-31	Issue for Review and Comment	A. H. Stretch	D. Wren, I. Love	
2	00-10-27	0	00-10-27	Issued as 'Approved for Use'	A. H. Stretch K. Reid	A.L. Wight	J. Hopwood
3		1D1	02-04-03	Issue for Review and Comment	C. Xu	A. H. Stretch	M. Bonechi
4		1D2	02-09-11	Issued for Review and Comment Incoporating the latest ACR design changes (e.g., eliminating the "Group"concept, updating ASI, etc)	W. Rabbani C. Nie	S.D. Nam A. Stretch V. Snell K. Hau E. Choy A. Josefowicz J. Millard M. Elgohary R. Ghai/O. Hines H. Shapiro H. Johal	
5		1	02-10-15	Issued as "Approved for Use".	W. Rabbani C. Nie	S.D. Nam A. Stretch V. Snell K. Hau	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	108	03650	SDG	001	1	3	

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
Safety Related Systems	65

CONTROLLED - CONTRÔLÉ

Release and Revision History / Liste des documents et des révisions

Release Document No./N°	Release Document Date	Revision Révision No./N°	Revision Révision 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
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.	W. Rabbani C. Nie	E. Choy A. Josefowicz J. Millard M. Elgohary R. Ghai/O. Hines H. Shapiro H. Johal 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	108	03650	SDG	001	2	3	

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
Safety Related Systems	65

CONTROLLED - CONTRÔLÉ

Release and Revision History / Liste des documents et des révisions

Release Document No./N°	Release Document Date	Revision Révision No./N°	Revision Révision 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	04-03-26	Issued as "Approved for Use". Revised technical changes consist of the following: -Underlined text in ASI 33540, 34320, 37000, 63108 in Table 1, ASI 21000, 32100, 33310, 33540, 34110, 34340, 35200, 35300, 36310, 53000, 63108, 66600, 68570, 71900, 751200 in Table 2, and A.2, A.2.1, A.2.2, A.2.3, A.2.4 in Appendix A. -Added ASI 34320, 33540 in Table 3, ASI 37000 in Table 4, and new sections of 3.6, 3.6.1, and A.2.5. In addition, the following changes are made to reflect the latest ACR design. These minor changes are not underlined and they consist of the following: -Removed ASI 36820, 33120, 35520, 36820, 63105, 63107, 65400, 68430, 68910, 71410, 73150 and all sub-index of 354xx, 356xx, 531xx, 532xx, 533xx, 534xx, 535xx, 732xx, 733xx, 785xx in the document, ASI 34410 in Table 3, and ASI 21000, 24000, 25000, 26001, 28007, 35360, 62030, 74000, and sub index of 357xx, 678xx in Table 4. -Updated description of the system, structure, and component to be consistent with the latest ASI description document. -Minor editoral changes through out the document.	P. Chan	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	108	03650	SDG	001	3	3	

TABLE OF CONTENTS

SECTION **PAGE**

TABLES

FIGURES

APPENDICES

TABLE OF CONTENTS

SECTION **PAGE**

1. PURPOSE

This Safety Design Guide identifies the safety related systems and structures which perform safety functions during normal plant operation and accident conditions, and the major safety requirements imposed on each identified system and structure. The Safety Design Guide applies to both NSP and BOP systems and structures.

2. COMPLIANCE

Compliance with Safety Design Guides is mandatory. A listing of Safety Design Guides is included in Appendix B. Deviations from the requirements identified in the guide may be allowed after they are reviewed and approved by completion of a Safety Design Guide Supplement, AECL form 0729-00.

3. SAFETY RELATED SYSTEMS

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

3.1 General

The safety objective for the design of a nuclear power plant is to protect the public and plant workers from adverse health effects due to the release of radioactive materials, during normal plant operation and during accident conditions.

To ensure safety, the following fundamental nuclear safety functions (Control, Cool, Contain and Monitor) shall be performed during operational states, during and following a design basis accident and, to the extent practicable, during and after the occurrence of plant conditions considered, to be beyond those of the design basis accident:

a) shut the reactor down and maintain it in a safe shutdown condition (Control),
b) remove heat from the fuel (Cool),
c) limit the release of radioactive material by maintaining a barrier (Contain), and
d) monitor the condition of the plant and perform actions necessary to maintain the above safety functions (Monitor).

Each of the above safety functions may be performed by several different safety related systems and structures. The specific systems and structures selected to perform the safety functions must satisfy various safety requirements, as identified in the Licensing Basis Document and Safety Design Guides.

3.2 Identification of Safety Related Systems

CSA N286.0 "Overall Quality assurance Program Requirements for Nuclear Power Plants"(Reference [1]) defines safety related systems as:

"*…those systems, and the components and structures thereof, which, by virtue of failure to perform in accordance with the design intent, have the potential to impact on the radiological safety of the public or plant personnel from the operation of the nuclear power plant. Those systems, and the components and structures thereof, are associated with:*

a) the regulation (including controlled startup and shutdown) and cooling of the reactor core under normal conditions (including all normal operating and shutdown conditions);
b) the regulation, shutdown, and cooling of the reactor core under anticipated transient conditions, accident conditions, and the maintenance of the reactor core in a safe shutdown state for an extended period following such conditions; and
c) limiting the release of radioactive material and the exposure of plant personnel and/or the public to meet the criteria established by the licensing authority with respect to radiation exposure during and following normal, anticipated transient conditions and accident conditions…"

Any system or structure directly or indirectly performing the safety functions outlined in Sections 3.1 and 3.2 above should be identified as a "safety related system or structure". Reference [1] further identifies the safety related *activities* as follows:

"...The term "safety related" also applies to certain activities associated with the design, manufacture, construction, commissioning, and operation of safety-related systems and to other activities which could similarly affect the radiological safety of the public or plant personnel, such as environmental and effluent monitoring, radiation protection and dosimetry, and radioactive material handling (including waste management). The larger the potential radiological safety effect associated with the performance of the activity, the stronger the "safety-related" connotation..."

3.3 Categorization of Safety Related Systems

In general, two categories of safety related systems and structures, Preventative or Protective, exist in a nuclear plant, as follows:

1) Preventative: systems and structures that perform safety functions during the normal operation of the plant, to ensure that radioactive materials remain within their normal boundaries. These are systems and structures whose failure could cause a release exceeding the regulatory dose limits for normal plant operation, in the absence of further mitigating actions, or whose failure as a consequence of an event could impair the safety functions of other safety related systems and structures.

   These Preventative systems and structures may be of the following types:

   1a) Systems or structures whose failure may cause a radioactive release to the public, in excess of the allowable normal release, in the absence of further protective action (e.g., heat transport system).

   1b) Systems or structures designed without further protective system lines of defence, whose failure may cause a radioactive release, in excess of the allowable normal release, to the public (e.g., spent fuel bay outside of containment).

   1c) Systems designed to prevent normal plant operations from leading to failures requiring further protective action, and required to:

   - control reactor power in the normal way,
   - shut down the reactor in the normal manner, or
   - remove decay heat in the normal manner.

   1d) Those parts of the plant whose failure during certain defined incidents could indirectly cause a radioactive release or adversely affect the operation of a safety related system and structure.

2) Protective: systems and structures that perform safety functions to mitigate events caused by failure of the normally operating systems or by naturally occurring phenomena. These systems and structures are of three types:

   2a) Systems designed to quickly shut down the nuclear reaction in the event of the failure of a normally operating safety related system or structure of the type discussed in 1(a) above.

2b) Systems and structures designed to remove decay heat and limit the radioactive release subsequent to the failure of a safety related system or structure, as discussed above.

2c) Systems and structures required to support proper operation of the protective systems and structures defined above. These systems and structures may have normal process functions as well (e.g., service water, electrical power).

The Protective systems and structures defined above are further identified as:

- Safety Systems, which are Shutdown System One, Shutdown System Two, Emergency Core Cooling, and Containment.
- Safety Support Systems, which provide services needed for proper operation of the Safety Systems (e.g., electrical power, cooling water). These systems may have normal process functions as well.

3.4 Safety Function Categorization System

Generally, the CANDU® safety related systems have been categorized as per the methodology described in Section 3.3 into Preventative and Protective types of safety system categories (1a to 1d and 2a to 2c, respectively). The safety related systems and structures are identified in Table 1 and their specific safety function and the major safety requirement are listed in Tables 2, 3 and 4.

3.5 Systems' Safety Functions

Table 1 lists all plant systems and structures, taken from the latest revision of the AECL Subject Index (ASI) list applicable for the ACR™*. The safety related systems and structures are identified, with their specific safety functions and major safety requirements, in Tables 2, 3 and 4. As the safety analyses and PSA are completed during the course of the project, additions or deletions to these lists may be justified.

The systems selected to perform the major safety functions of reactor shutdown, heat removal from the fuel, containment, and monitoring and control are outlined in Appendix A, with a brief description of their specific functions.

Appendix A provides a conceptual description of the safety functions of the major safety related systems and structures and an overview of the transfer of residual heat from the reactor to the ultimate heat sinks. This description is provided for information only, and does not impose any special requirements on the ACR systems.

3.6 Safety Design and Analysis Basis

The ACR-700 safety analysis demonstrates that the operation of the plant does not pose an unacceptable radiological risk to the off-site public, on-site plant staff, or the environment as a consequence of an abnormal event. The safety analysis approach is based on the risk-informed concept that the most probable occurrences should yield the least radiological consequences, and situations having the potential for the greatest consequences should be least likely to occur. Within the safety analysis framework, a spectrum of events is defined and classified, and an

---

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

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

appropriate analysis method is selected. The ACR Safety Basis Document (Reference [2]) defines and elaborates the safety analysis approach.

The safety analysis covers the five classification of events, which include "Design Basis Events" or DEs, (Class 1, Class 2 and Class 3), and two "Limited Core Damage Accidents" or LCDAs, (Class 4 and Class 5). Each event has a probabilistic frequency of occurrence and an associated acceptance criterion in terms of the dose limit. In addition, a category of extremely improbable events that lead to loss of core geometry is also defined and is referred to as "Severe Core Damage Accidents" or (SCDAs).

The design basis events (i.e. Classes 1 to 3) establish the design requirements for engineered safety features in the mitigation systems. The safety analysis approach is based on conservative assumptions and assumes a single failure in a mitigating system occurring simultaneously with an initiating event.

The safety analysis for LCDAs (i.e. Classes 4 and 5) uses design-centred assumptions. Systems and equipment credited in the safety analysis are assessed to provide reasonable assurance of their capability to operate on a case-by-case basis via design assessments. The safety analysis is performed using detailed analysis models.

The safety analysis for SCDAs uses design-centred assumptions. A Level 2 Probabilistic Safety Assessment (PSA) using integral models is employed in the safety analysis.

3.6.1 Single Failure Criterion

The ACR safety design approach requires that the mitigating systems have sufficient independence and redundancy to perform their safety functions assuming a single failure (Reference [2]). The mitigating systems are systems that meet the control, cool, and contain safety functions for the design basis events; these systems are identified in the Single Failure Criterion (SFC) Design Guide. The auxiliary supporting features to these systems are also subjected to the U.S. SFC. The design guide provides information on the rules/practices to design these systems to meet the SFC. Analysis such as a Failure Mode and Effect Analysis (FMEA) is required to demonstrate that mitigating systems meet the SFC. The SFC assessment also includes identification of a limiting single failure in the system. The limiting single failure is the failure that has the worst consequence to the system's performance. This failure is integrated into the conservative assumption for DEs when the safety analysis is performed.

4. SAFETY REQUIREMENTS FOR SYSTEMS AND STRUCTURES

a) The designer shall ensure that the relevant safety requirements identified in Tables 2, 3, and 4 are addressed in design and analysis documents in more detailed quantitative terms, as necessary, to define the detailed design.

b) The functions and requirements included in Table 2 shall be confirmed during the design process by means of PSA and/or safety analyses.

c) During the design process, any additional systems and structures which satisfy the criteria outlined in Section 3.2 shall be identified in design documentation as being safety related, the appropriate safety requirements shall be included in the Design Requirements documents, and shall be added to Tables 2, 3, or 4.

   Such systems and structures may be identified by the safety analyses or probabilistic analyses for the project, or they may provide support services to an identified safety related system or structure which is essential to the performance of its safety function, or they may be interfacing systems or structures which could impair the required safety function of a safety related system or structure.

d) Systems and structures, which form part of the containment boundary are listed in Table 3 and shall satisfy the requirements given in Safety Design Guide 108-03650-SDG-006.

e) Systems or structures which contain radioactive materials or which monitor the presence of radioactive materials are listed in Table 4. The type and amount of radioactive materials shall be considered in pressure boundary code classification and in radiation protection design.

f) The events and safety functions included in Table 2 are for information only and are not comprehensive; the more specific events included in Regulatory Documents, the Systematic Review of the Plant Design, and preliminary PSA studies shall be used for design purposes, with corresponding detailed safety functions and safety requirements for each system.

g) As required by CNSC document S-98 (Reference [3]), the functions of the safety-related systems or structures identified in Tables 2 and 3 shall be confirmed by safety analyses/assessment. The designer shall:

   1) Identify how each system contributes to the overall safety objectives of the plant.
   2) Identify the system or structure performance necessary to carry out the safety functions.
   3) Assign reliability targets that will ensure that each system or structure can achieve its safety function.
   4) Design the system or structure so it is possible to demonstrate, during plant operation, that the systems or structures can meet their performance requirements by testing, inspection, monitoring, or other measures.

h) Safety related systems or structures that perform safety functions during normal plant operation, shall be designed to minimize the frequency of process failures which would lead to exceeding the dose limits for normal plant operation in the absence of further mitigating actions.

5. DOCUMENTATION

a) The safety function, and specific design requirements arising from the function, shall be described in the design requirement documents for each safety related system and shall cross reference the safety design guide requirement.

b) Design documentation to confirm the safety functions and performance requirements for each safety related system shall be provided to satisfy the requirements of CNSC S-98 (Reference [3]).

c) A list of safety related systems shall be established and maintained, describing the safety related function and the reason that it is required.

6. REFERENCES

[1] CSA N286.0, “Overall Quality Assurance Program Requirements for Nuclear Power Plants”.

[2] 108-03600-AB-003, “Safety Basis for ACR”.

[3] CNSC S-98, “Reliability Programs for Nuclear Power Plants”.

[4] CNSC R-7, “Requirements for Containment System for CANDU Nuclear Power Plants”.

[5] CNSC R-77, “Overpressure protection Requirements for Primary Heat Transport System in CANDU Power Reactor Fitted with Two Shutdown Systems”.

[6] CNSC R-9, “Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants”.

[7] CSA N290.4, “Requirements for the Reactor Regulating Systems of CANDU Nuclear Power Plants”.

[8] CNSC R-8, “Requirements for Shutdown Systems for CANDU Nuclear Power Plants”.

[9] CAN3-N290.6, “Requirements for Monitoring and Display of CANDU Nuclear Power Plant Status in the Event of an Accident”.

[10] CAN/CSA N293, “Fire Protection for CANDU Nuclear Power Plants”.

[11] CNSC R-10, “The Use of Two Shutdown Systems in Reactors”.

[12] CAN3 N290.1, “Requirements for the Shutdown Systems of CANDU Nuclear Power Plants”.

Table 1
List of ACR Systems and Structures

The following is a preliminary listing of the systems and structures included in the design of the proposed ACR plant. Safety related systems or structures are identified in the following list by reference to Tables 2, 3, or 4, which outline the major safety requirements to be satisfied in design. Where no safety requirements were identified at the time of writing of this safety design guide, the system is designated as "Not Safety Related", shown as NSR in the list.

Brackets are used to provide necessary descriptive information (e.g., moderator) that is not part of that specific ASI.

ASI	System or Structure	Safety Requirement
20000	**BUILDINGS AND STRUCTURES**	
21000	REACTOR BUILDING	Table 2
21600	Special Equipment (Airlocks, Shielding Doors, Blowout Panels, Atmosphere Barriers, Equipment Hatch) (also see ASI 68400)	Tables 2, 3 and 4
22000	TURBINE BUILDING	Table 2
23000	COOLING WATER STRUCTURES	
23003	Condenser Cooling Water Pumphouse	NSR
23005	Raw Service water Pumphouse	Table 2
24000	REACTOR AUXILIARY BUILDING (Note: Long-Term Cooling pumps and Heat Exchangers are assumed to be located in the Reactor Auxiliary Building)	Table 2
24250	Spent Fuel Bay	Tables 2 and 4
25000	CONTROL BUILDINGS (MCR, SCA)	Table 2
26001	Maintenance Building (Note: New Fuel (see 35100) are assumed to be located in the Maintenance Building)	NSR
26005	Service Building	NSR
27000	PROJECT STRUCTURES (including Administration Building)	NSR
28000	AUXILIARY STRUCTURES	
28001	Transformer Area Structures	NSR

ASI	System or Structure	Safety Requirement
28002	Switchyard Area Structure	NSR
28003	Standby Generator Area Structure	Table 2
28005	Water Treatment Structure	NSR
28006	Sewage Treatment Structure	NSR
28007	Radioactive Waste Storage Structure	NSR
28008	Heavy Water Upgrading Structure	NSR*
29000	ANCILLARY STRUCTURES (Guardhouse, Oil Storage, Fresh Water Supply, Compressed Gas Storage, Vehicle Maintenance and Storage)	NSR
30000	**REACTOR, REACTOR SYSTEMS, AND AUXILIARIES**	
30100	Nuclear Safeguards System and Equipment	(see specific system) Table 4
30700	Special and Consumable Materials	(see specific system) Table 4
30800	Process Systems Components	(see specific system) Table 4
30900	Miscellaneous Components for Nuclear Process Systems	(see specific system) Table 4
31000	REACTOR	Tables 2 and 4
31100	Fuel Channel Assemblies	(see 31000)
31200	Calandria Shield Tank Assembly	(see 31000)
31700	Reactivity Control Units	(see specific system) Table 4
31710	Reactivity Mechanisms Deck	(see 31000)
31730	Shutoff Units	See 63700, 68200
31740	In-Core Flux Detector Units	See 63700, 68200, 68300
31750	Zone Control Units	See 63700
31760	Liquid Injection Shutdown Units	See 63700, 68300
31770	Solid Control Absorber Units	See 63700
31790	Ion Chamber Units	See 63700, 68200, 68300
31800	Reactor Shielding	(see specific system) Table 4

* Failure shall not affect the function of safety related systems.

ASI	System or Structure	Safety Requirement
31900	Installation and Maintenance Equipment	NSR, Table 4
32000	MODERATOR SYSTEMS AND AUXILIARIES	
32100	Moderator Systems	Tables 2 and 4
32210	(Moderator) Purification System	Tables 2 and 4
32300	(Moderator) Cover Gas System	Tables 2, 3 and 4
32500	(Moderator) Heavy Water Collection Systems	Tables 3 and 4
32600	(Moderator) Heavy Water Sampling Systems	Tables 3 and 4
32700	(Moderator) Liquid Poison Systems	Tables 2 and 4
33000	HEAT TRANSPORT SYSTEMS AND AUXILIARIES	
33100	Heat Transport System	Tables 2 and 4
33300	Heat Transport System Auxiliaries	See below
33310	Heat Transport Pressure and Inventory Control System	Tables 2 and 4
33340	Heat Transport Pump Seal System	Tables 2 and 4
33350	Heat Transport Purification System	Tables 2 and 4
33500	Gas Control System	See below
33530	Heat Transport Nitrogen Addition System	Table 3
33540	Heat Transport Hydrogen Addition System	Tables 2 and 3
33710	Heat Transport Sampling System	Tables 3 and 4
33810	Heat Transport Collection Systems	Tables 3 and 4
33900	Installation and Maintenance Equipment (Feeder Freezing)	NSR
34000	AUXILIARY SYSTEMS	
34100	Cooling Systems	See below
34110	Shield Cooling System	Tables 2 and 4
34300	Emergency Core Cooling System and Reserve Water System	See below
34320	Emergency Coolant Injection System	Tables 2, 3 and 4
34340	Reserve Water System	Table 2
34350	Long-Term Cooling System	Tables 2, 3 and 4
34400	Spent Fuel Bay Systems	See below
34410	(Spent Fuel Bay) Cooling and Purification System	Tables 2 and 4
34500	Resin Transfer Systems	See below
34510	Resin Transfer System	Tables 3 and 4
34700	Liquid Injection Shutdown	See below
34710	Liquid Injection Shutdown System	Tables 2 and 4
34900	Miscellaneous Reactor Process Systems	See below

ASI	System or Structure	Safety Requirement
34980	Annulus Gas System	Tables 2 and 4
35000	FUEL HANDLING AND STORAGE	
35100	New Fuel Transfer and Storage	Tables 2, 3 and 4
35110	New Fuel Transfer	See 35100
35120	New Fuel Storage and Handling	See 35100
35130	New Fuel Transfer Auxiliaries	NSR
35200	Fuel Changing	Tables 2, 3 and 4
35210	Fuelling Machine Head	(see 35200)
35220	Fuelling Machine Bridge/Carriage	(see 35200)
35230	Fuelling Machine Water Systems	(see 35200)
35250	Fuelling Machine Gas Auxiliary Systems	(see 35200)
35260	Fuelling Machine Emergency Water Systems	(see 35200)
35300	Spent Fuel Transfer and Storage	Tables 2, 3 and 4
35310	Spent Fuel Discharge	(see 35300)
35320	Spent Fuel Transfer Auxiliaries	(see 35300)
35330	Spent Fuel Transfer Equipment	(see 35300)
35360	Storage Bay	Table 2
35400	Spent Fuel Shipping	NSR
35500	Reactor Component Handling	See below
35510	Fuel Channel Component Handling Tools	Table 4
35600	Maintenance and Service Facilities	NSR
35700	Fuelling Machine Transfer	NSR
35710	Fuelling Machine Maintenance Lock Equipment	NSR
35730	FM Cable and Hose Management System	Table 2
36000	STEAM GENERATOR SYSTEMS	
36100	Steam and Relief Systems	Tables 2 and 3
36110	Main Steam and Water System (FEEDWATER PORTION OF SYSTEM IS AN EXTENSION OF ASI 43230)	(see 36100)
36140	Main Steam Pressure Control and Relief System	(see 36100)
36300	Steam Generator Auxiliary Systems	(see 36100)
36310	Steam Generator Blowdown System	Tables 2 and 3
36400	Controlled Steam Discharge Systems - Blowoff	Table 3
36410	Controlled Steam Discharge Circuit	(see 36400)
36500	Steam Dump to Condenser	NSR
36600	Steam Generator Water Sampling System	Table 3
36700	Steam Sampling	NSR

ASI	System or Structure	Safety Requirement
36800	Ancillary Steam Systems	NSR
36900	H_2O Leakage Collection System	NSR
37000	FUEL	Tables 2 and 4
37100	Out-Reactor Testing	(see 37000)
37200	In-Reactor Testing	(see 37000)
37300	Fuel Manufacture	(see 37000)
38000	WATER MANAGEMENT	
38100	Water Supply System	Tables 3 and 4
38310	Heavy Water Vapour Recovery System	Tables 3 and 4
38900	Auxiliary and Support Systems	(See below)
38910	Miscellaneous Heavy Water Collection	Table 4
38920	Heavy Water Sorting Station	Table 4
38930	Drum Cleaning Facilities	Table 4
40000	**TURBINE-GENERATOR AND AUXILIARIES**	
41000	TURBINE GENERATOR	NSR
41100	Turbine and Auxiliary Equipment	NSR
41200	Generator and Auxiliary Equipment	NSR
41300	Oil Systems	NSR
41500	Turning Gear	NSR
41600	Oil Fire Protection System	Table 2
42000	CONDENSING SYSTEMS	NSR
42110	Condenser System	NSR
42120	Extraction Air System	NSR
43000	FEEDWATER AND AUXILIARY STEAM SYSTEMS	
43100	Feedwater Heating System	NSR
43200	Condensate and Feedwater Systems	see specific ASI below
43210	Condensate System	NSR
43220	Condensate Makeup and Rejection System	NSR
43230	Feedwater System	Tables 2 and 3
43240	Condensate Purification System	NSR
43300	Auxiliary Steam Systems	NSR
45000	AUXILIARY SYSTEMS	(see below)

ASI	System or Structure	Safety Requirement
45100	Sampling System	NSR
45200	Steam Drain System	NSR
45400	Chemical Control Systems (Hydrazine, Amine, Phosphate)	NSR
50000	**ELECTRIC POWER SYSTEMS**	
50000	ELECTRIC POWER SYSTEM	Table 2
51000	MAIN STATION CONNECTION	(see 50000)
51100	High Voltage System No. 1 (380 kV or higher)	(see 51000)
51400	High Voltage System No. 4 (Main Generator – less than/or 24 kV)	NSR
52000	STANDBY GENERATORS	Table 2
52100	Generator and Auxiliaries	(see 52000)
52200	Prime Mover and Auxiliaries	(see 52000)
53000	DISTRIBUTION SYSTEM	Table 2
53100	Voltage Level No. 1 (12 or 15 kV AC Class)	NSR
53200	Voltage Level No. 2 (5 or 7 kV AC Class)	(see 53000)
53300	Voltage Level No. 3 (380 V, 480 V, 600 V AC Class)	(see 53000)
53400	Voltage Level No. 4 (220 V AC and less)	(see 53000)
53500	Voltage Level No. 5 (250 V DC typical)	(see 53000)
56000	LIGHTING AND BUILDING SERVICE SYSTEMS	Table 2
56100	Reactor Building Systems	(see 56000)
56200	Turbine Building Systems	(see 56000)
56300	Condenser Cooling Water Pumphouse	(see 56000)
56400	Reactor Auxiliary Building	(see 56000)
56500	Main Control Building	(see 56000)
56600	Maintenance Building	(see 56000)
56700	Administration Building	(see 56000)
56800	Auxiliary Structures	NSR
56900	Ancillary Structures	NSR
57000	CABLING SYSTEM	Table 2 (see specific system)
57100	Power Cables	(see specific system)
57200	Instrumentation and Control Cables	(see specific system)
57300	Special Cable	(see specific system)

ASI	System or Structure	Safety Requirement
57400	Cable Trays	(see specific system)
57500	Junction Boxes	(see specific system)
57600	(Electrical) Containment Penetrations	Tables 2 and 3
57700	Conduit and Fittings	(see specific system)
57800	Underground Cable Ducts, Manholes and Trenches	(see specific system)
58000	GROUNDING AND CATHODIC PROTECTION	NSR
58200	Grounding - Equipment and Buildings	NSR
58300	Instrument System Grounding	NSR
58400	Cathodic Protection	NSR
58700	Lightning Protection and Shielding	NSR
60000	**INSTRUMENTATION AND CONTROL**	
60030	Vibration Monitoring and Alarm Systems	NSR
60200	Communications	NSR
60300	Annunciation	(see specific system)
60400	Instrument Hardware (Bulk Order)	(see specific system)
60500	Instrument Test and Calibration Equipment	NSR
60600	Instrument Installation	(see specific system)
60700	Common Field Panels and Racks	(see specific system)
60800	Common Electrical Connections	(see specific system)
61000	SITE INSTRUMENTATION SYSTEMS	
61100	Environmental Monitoring Equipment	NSR
61200	Meteorological Monitoring Equipment	NSR
61300	Radiation Monitoring and Sampling Equipment	Table 4
61400	Site Security Equipment	NSR
61500	Seismic Instrumentation Equipment	Table 2
62000	BUILDING AND STRUCTURES INSTRUMENTATION	
62030	Access Control System	NSR
62100	Reactor Building Instrumentation	NSR
62161	Airlocks	(See 67314)
62200	Turbine Building Instrumentation	NSR
62300	Cooling Water Structures Instrumentation	NSR
62400	Reactor Auxiliary Building Instrumentation	NSR
62500	Control Building Instrumentation	NSR
62600	Services Buildings Instrumentation	NSR
62700	Project Structures Instrumentation	NSR

ASI	System or Structure	Safety Requirement
63000	REACTOR, REACTOR SYSTEMS AND AUXILIARIES SYSTEMS	
63100	Reactor Instrumentation	(see specific system)
63101	Channel Flow Verification	Table 2
63102	Channel Temperature Monitoring	Table 2
63103	Gaseous Fission Product Monitoring	Tables 2 and 4
63108	Failed Fuel Detection (System)	Tables 2 and 4
63120	Calandria and End Shield Instrumentation	NSR
63200	Moderator Systems	(see 32000)
63300	Heat Transport Systems	(see 33000)
63400	Auxiliary Systems	(see 34000)
63500	Fuel Handling Control	(see 35000)
63600	Steam Generator Systems	(see 36000)
63700	Plant Control	Table 2
63800	Water Management	(see 38000)
63862	Heavy Water in Light Water (Leak Detection)	Table 3
64000	TURBINE GENERATOR AND AUXILIARIES	
64100	Turbine Generator	NSR
64200	Condensing Systems	NSR
64300	Feedwater and Auxiliary Steam Systems	(see 43000)
64500	Auxiliary Systems	NSR
65000	CONTROL OF ELECTRIC POWER SYSTEMS	
65100	Main Station Connections	(see 50000 series)
65200	Standby Generators	(see 50000 series)
65300	Service Distribution	(see 50000 series)
65600	Lighting and Building Service Systems	(see 50000 series)
65800	Grounding and Cathodic Protection	(see 50000 series)
66000	CONTROL CENTRE	Table 2
66100	Main Control Room (MCR)	see 66000
66200	Control Equipment Room	see 66000
66300	Safety System Monitor Computers (SSMC)	see 66000
66400	Fuel Handling Display System	see 66000
66500	Plant Display System	see 66000
66600	Secondary Control Area (SCA)	Table 2
66700	Distributed Control System	See 66000

ASI	System or Structure	Safety Requirement
66800	Fuel Handling Distributed Control System	NSR
66900	Simulation	NSR
67000	COMMON PROCESSES AND SERVICES	
67100	Water Systems	(see 70000 series)
67147	Fire Detection and Alarm System	Table 2
67300	Heating, Cooling, and Ventilation Systems	(see 70000 series)
67314	Containment Isolation	Tables 2 and 3
67400	Miscellaneous Common Services	(see 70000 series)
67500	Compressed Gases	(see 70000 series)
67600	Material Handling System	NSR
67700	Maintenance Facilities	NSR
67800	Miscellaneous Systems and Equipment	NSR
67857	Radiation Protection Equipment	Table 3
67900	Radioactive Waste Management	(see 79000)
68000	SAFETY SYSTEMS	
68200	Shutdown System No. 1 (SDS1)	Tables 2 and 3
68300	Shutdown System No. 2 (SDS2)	Tables 2 and 3
68400	Containment System (See 67314 for Containment Isolation)	Tables 2 and 3
68440	Containment Ventilation Isolation System	Tables 2, 3 and 4
68470	Gross Leakage Monitoring	(see 68400)
68480	Hydrogen Control System	Tables 2 and 3
68500	Emergency Core Cooling	(see 34320, 34350)
68570	Second Crash Cooldown System	Table 2
68900	Post Accident Management	Table 2
70000	**COMMON PROCESSES AND SERVICES**	
71000	WATER SYSTEMS	
71100	Pumphouse Systems	(see 71300)
71110	Common Services Water Systems	(see 71300)
71120	Trash Removal System	(see 71310)
71200	Condenser Cooling Water Systems	NSR
71300	Service Water Systems	(see below)
71310	Raw Service Water System	Table 2
71340	Recirculated Cooling Water System	Tables 2 and 3
71400	Fire Water Protection System (Fire Water Supply System)	Tables 2 and 3

ASI	System or Structure	Safety Requirement
71500	Domestic Water System	NSR
71600	Water Treatment Plant	NSR
71650	Demineralized Water System	Table 3
71700	Sewage and Drainage System	NSR
71730	Active Drainage Reactor Building	Tables 3 and 4
71740	Active Drainage Reactor Auxiliary Building and Services Building	Table 4
71800	Chlorination	NSR
71900	Chilled Water System	Tables 2 and 3
72200	Fuel Oil Systems	Table 2
73000	HEATING, COOLING, AND VENTILATION SYSTEMS	
73010	Building Heating Plant	NSR
73100	Reactor Building (HVAC)	(see below)
73110	(Reactor Building) Cooling System	Tables 2 and 3
73120	(Reactor Building) Ventilation System	Tables 2, 3 and 4
73140	Containment Isolation	Tables 2 and 3
73200	Turbine Building (HVAC)	NSR
73300	Cooling Water Structures (HVAC)	(see below)
73310	Condenser Cooling Water Pumphouse Heating System	NSR
73320	Condenser Cooling Water Pumphouse Ventilation System	NSR
73350	RSW Pumphouse Heating System	Table 2
73360	RSW Pumphouse Ventilation System	Table 2
73400	Reactor Auxiliary Building (HVAC)	(see below)
73410	(RAB) Heating System	Table 2
73420	(RAB) Ventilation System	Table 2
73440	Decontamination Centre Ventilation	Table 4
73470	Spent Fuel Bay Ventilation System	Table 4
73500	Control Building	(see below)
73510	Main Control Building (HVAC)	Table 2
73520	Secondary Control Area (HVAC)	Table 2
73600	Service Buildings (HVAC)	NSR
73800	Auxiliary Structures (HVAC)	NSR
73900	Miscellaneous Structures (HVAC)	Table 2
74000	MISCELLANEOUS COMMON SERVICES	NSR

ASI	System or Structure	Safety Requirement
75000	COMPRESSED GASES	
75100	Compressed Air System	(see below)
75110	Plant (Service) Air System	Table 3
75120	Instrument Air System	Tables 2 and 3
75130	Breathing Air System	Table 3
75140	HP Air Supply System	(see 75120)
75200	Carbon Dioxide Systems	NSR
75300	Hydrogen Circuit	Table 3
75500	Oxygen System	Table 3 (for moderator cover gas)
75600	Combustible Gases	Table 2
75700	Nitrogen (System)	Table 3
76000	MATERIAL HANDLING	Table 2
76010	Cranes and Hoists - Reactor Building	(see 76000)
76030	Cranes and Hoists - Other Buildings	(see 76000)
77000	MAINTENANCE FACILITIES	NSR
78000	MISCELLANEOUS SYSTEMS AND EQUIPMENT	
78100	Auxiliary Steam and Condensate - Feedwater System	NSR
78200	Fuel Oil Systems	Table 2
78500	Miscellaneous Equipment	NSR
78580	Administration Building	NSR
79000	RADIOACTIVE WASTE MANAGEMENT	Table 2
79100	Solid Wastes	Table 4
79140	Solid Waste Spent Resin Management System	Tables 3 and 4
79210	Liquid Waste Management System	Table 4
79310	(Gaseous Wastes) Discharge System	Tables 3 and 4
79320	Offgas Waste Management System	Tables 3 and 4
80000	**CONSTRUCTION**	**NSR**

Table 2
Safety Requirements for Systems and Structures

The safety functions and major safety requirements are shown in this Table 2 for the Safety Related Systems and Structures identified in Table 1. The events for which these safety functions are required are shown in a more detailed manner in the Final Safety Analysis Report. The safety functions and requirements are shown in general terms, more detailed or additional requirements would be identified during design, arising from safety analyses and PSA, and will be shown in the design requirements documents.

The safety categories either **1 (a), (b), (c), (d) or 2 (a), (b), (c)** assigned in the Table are based on the Preventative or Protective type of safety related systems defined in Section 3.3.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
20000		BUILDING AND STRUCTURES		
21000	1(d), 2(b) (See 68400)	Reactor Building	Barrier to the release of radioactive materials following a release within the containment envelope.	The reactor building (RB) shall be designed with a leak rate which will satisfy public dose criteria for events involving releases of radioactive materials inside the building.
			Protection of safety related systems from environmental conditions and severe events occurring outside the RB.	The RB shall be designed for an internal highest pressure and temperature caused by a LOCA, combined with a limiting single failure of a mitigating system.
			Support of safety related systems inside the RB (internal structures).	The RB shall retain its structural integrity for all internal and external design basis events, including a MSLB combined with a limiting single failure of a mitigating system, to enable safety related components to continue to function as required. There shall be no damage to containment structure for all design basis events with LACs available, including main steam line break. The RB layout shall enable safety related systems and components which are required to perform an active safety function to be located above the internal flood level for events which release coolant within the building. The requirements of CNSC Regulatory Document R-7 (Reference [4]) shall be satisfied. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
21600	1(d), 2(b)	Special Equipment (Airlocks, Shielding Doors, Blowout Panels, Atmosphere Barriers, Equipment Hatch)	Barrier to the release of radioactive materials Protection of plant staff from radiation exposure	The containment airlocks and equipment hatch shall be qualified for LOCA and MSLB to maintain their seals. For airlocks, provisions shall be made for their manual operation after a DBE. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 005, 006, 007.
22000	1(d)	Turbine Building	Protect safety related systems from the consequences of events occurring in the Turbine Building (TB).	The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005. (Note: design intent should be to minimize safety related systems in the TB, and to ensure that no Safety Support systems are located in the TB)
23005	1(d)	Raw Service Water Pumphouse	Protect safety related systems against the effects of external events and provide acceptable environmental conditions for systems and components housed within.	Physical separation shall be provided to ensure that external events or component failures in the other areas of the plant do not impair the safety function of the safety related systems. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 004, 005.
24000	1(d)	Reactor Auxiliary Building (Note: Long-Term Cooling system is located in the Reactor Auxiliary Building)	Protect safety related systems against the effects of external events and provide acceptable environmental conditions for systems and components housed within.	Physical separation shall be provided to ensure that external events or component failures in the other areas of the plant do not impair the safety function of safety related systems. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005.
24250	1(b)	Spent Fuel Bay	Heat removal from spent fuel. Prevention of radioactive release.	The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 004, 005, 007.
24xxx	1(d)	MSSV/MSIV Structure	Protect safety related components (MSSVs and MSIVs) from the effects of environmental conditions.	The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG- 002, 003, 004, 005.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
25000	1(d)	Control Building	Protect safety related systems against the effects of external events and provide acceptable environmental conditions for systems and components housed within.	The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 004, 005.
28003	1(d)	Standby Generator Area Structure	Protect safety related systems against the effects of external events and provide acceptable environmental conditions for systems and components housed within.	The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG- 002, 004, 005.
30000	REACTOR, REACTOR SYSTEMS AND AUXILIARIES			
31000	1(a), 1(d)	Reactor (see 32100 and 33100)	Maintain the integrity of the heat transport system and provide support for reactor control mechanisms.	The reactor structures shall retain their structural integrity for all events, to the extent that the reactor can be shut down and the fuel can be cooled. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 005, 007.
32000	MODERATOR SYSTEMS AND AUXILIARIES			
32100	2(c), 1(d)	Moderator System	Maintain the moderator at an appropriate subcooling margin.	The moderator system shall be capable of maintaining its system integrity following a design basis accident. The moderator system shall be capable of removing the heat from the fuel following a LCDA, such as LOCA combined with a loss of ECC system. Sufficient subcooling of the moderator and a suitable pump NPSH is required for LOCA+LOECC. Note that a review of the impact of loss of normal function should be considered for the moderator system.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
				The components within the containment envelope (reactor building) shall be environmentally qualified (see 108-03650-SDG-003). The materials used for the moderator system shall withstand the high radiation fields associated with an in-core LOCA. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 007.
32210	1(d)	(Moderator) Purification System	Maintain the shutdown condition of the reactor after SDS2 trip during accident conditions.	The purification process shall be stopped after events requiring reactor shutdown by means of SDS2, to avoid removing the poison from the moderator. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 007. To comply with Clause 4.1.1 of CNSC Regulatory Document R-8, the system shall provide at least two independent means of ensuring that reactor remains subcritical under a guaranteed shutdown state condition.
32300	1(d)	(Moderator) Cover Gas System	Maintain the integrity of the HTS. Maintain the fuel cooling capability of the moderator system.	Prevent the accumulation of explosive levels of deuterium in the calandria during normal plant operation. Maintain the subcooling conditions in the moderator to permit fuel cooling after a loss of coolant accident (also see 32100). The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-003, 005, 006, 007.
32700	2(c)	(Moderator) Liquid Poison System	Maintain the reactor in a shutdown condition.	For events in which SDS1 (ASI 68200) shuts the reactor down and SDS2 is unavailable, this system shall be designed to add negative reactivity through operator action. Operator action shall not be credited for at least 15 minutes. (Note: For in-core LOCA, SDS1 depth is not an issue for ACR due to light water in HT system inserting negative reactivity into moderator).

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
				The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-003, 007.
33000	HEAT TRANSPORT SYSTEMS AND AUXILIARIES			
33100	1(a), 2(b)	Heat Transport System	Maintain the capability to remove heat from the fuel, including via thermosyphoning.	For normal operation and accident events in which the heat transport system pressure boundary remains intact, the system shall be capable of removing the stored and decay heat to prevent fuel failures.
			During normal operation, provide a barrier to the release of radioactive materials to ensure that doses to plant staff remain within acceptable limits.	For events in which the HTS pressure boundary fails, the system shall, in conjunction with the mitigating systems such as ECC (emergency coolant injection + long-term cooling), limit the fuel damage to satisfy the regulatory criteria outlined in the Licensing Basis Document. The design shall consider the cases where the emergency core cooling is available or unavailable. The HTS pressure boundary shall be designed to withstand the forces and vibration resulting from continued main heat transport pumps operation after a LOCA, until the automatic pump trip is actuated. The design shall satisfy the overpressure protection requirements of CNSC Regulatory Document R-77 (Reference [5]). The design shall, in conjunction with the ECC system, satisfy the requirements of CNSC Regulatory Document R-9 (Reference [6]). The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 005, 007.
33310	1(c), 1(d)	Heat Transport Pressure and Inventory Control System	Maintain adequate inventory in the heat transport system to ensure fuel cooling during normal plant operation and anticipated operational occurrences.	The system shall maintain adequate inventory in the heat transport system to ensure heat removal from the fuel during normal plant operation and anticipated operational occurrences, and ensure thermosyphoning capability following loss of the main HT pumps due to loss of Class IV power.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
			Maintain the integrity of the primary HTS pressure boundary.	The rate of inventory makeup during normal plant operation shall be sufficient to permit continued fuel cooling despite leaks due to a SG tube failure, an individual instrument tube failure, or a FM cooling line failure.
			Maintain the suction pressure to the FM water supply pumps in order for the FM pumps to continue to supply fuel cooling flow to the FMs	Indication of HT inventory depletion due to leakage or spurious feed/bleed operation shall be provided in the MCR. Isolating valves on the HTS (e.g., feed and bleed valves or similar valves) shall ensure that the HTS pressure boundary integrity is maintained for all events (i.e. DE or LCDA). The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 007.
33340	1(d)	HT Pump Seal System	Maintain the integrity of the primary HTS pressure boundary.	The system shall provide cooling to the HT pump seals. The system shall stop discharge from the HTS for events in which gland seal cooling has failed or is not required. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 005, 007.
33350	1(d)	Heat Transport Purification System	Remove the radioactive substances from the reactor coolant, including activated corrosion products and fission products leaking from the fuel.	The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-007 Note: The system is assumed to be within the containment.
33540	1(d)	Heat Transport Hydrogen Addition System	None	The location and design of the system shall comply with fire protection requirements, as outlined in CAN/CSA N293 (Reference [10]). The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 005, 006.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
34000	AUXILIARY SYSTEMS			
34110	1(c), 1(d)	Shield Cooling System	Provide shield cooling to maintain reactor structure integrity	The shield cooling system shall be capable of removing heat accumulated in the reactor structure and shielding during normal operation and certain design basis events to ensure the calandria vessel is maintained at the appropriate stress level. For a SCDA, the water-filled shielding tank serves as a passive heat sink. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-003, 005, 007.
34300	Emergency Core Cooling System			
34320	2(b)	Emergency Coolant Injection System	Provide inventory make-up to the HTS in the short term (high-pressure injection stage) of a LOCA.	The system shall be capable of providing inventory make-up to the HTS for all sizes of HTS pressure boundary failures, and heat removal through the SGs for small breaks. The system shall also be capable of making up for shrinkage due to rapid cooling (e.g., MSLB event) with an intact pressure boundary, and of post-DBE make-up to the HTS for pre-existing leaks. The system shall be automatically actuated for all events where makeup or cooling is required within 15 minutes of the initiating event. HTS depressurization is required for coolant injection following small LOCA. The ECI system function shall be maintained despite loss of Class IV power. The system shall satisfy the requirements of CNSC Regulatory Documents R-7 (Reference [4]) and R-9 (Reference [6]). The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006, 007.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
34340	2(b), 2(c)	Reserve Water System	Store water for make-up to the HTS, the LTC system, moderator and shield tank, and as a backup FW supply for the SGs.	The system shall provide feedwater (FW) to the SGs following reactor shutdown for events where the SGs act as a heat sink, and for which both the main and Auxiliary Feedwater (AFW) supplies are unavailable. The system shall provide an emergency source of water to the containment sumps in the event of a LOCA to ensure net positive suction head for the LTC pumps. The system shall provide emergency makeup water by gravity to HTS. The system shall be capable of providing makeup to the moderator system, and shield cooling system for SCDAs. The system shall be initiated automatically for events where the steam generator inventory is depleted in less than 15 minutes (e.g., MSLB). Instrumentation for SG level control shall be provided, unless manual operator action is shown to be adequate (i.e., compatible with PSA operator model). The system shall be capable of supplying FW to the SGs until the LTC system can be introduced. The system shall satisfy the requirements of CNSC Regulatory Policy Statement R-9, including 2.2 (b) (Reference [6]). The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006.
34350	2(b)	Long Term Cooling System	Provide fuel cooling in the long term (recovery stage) of a LOCA. Remove decay heat indefinitely in the long term for transients and accidents with the HTS pressure boundary intact.	Following shutdown with the HTS pressure boundary intact, the system shall be capable of removing decay heat from the fuel for a long term. (Immediate heat removal following shutdown is provided by the SGs and associated FW systems.) The system shall be capable of removing heat by recovering, cooling, and re-injecting the coolant discharged from the break in the long term of a LOCA.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
				The system shall be automatically actuated for all events where makeup or cooling is required within 15 minutes of the initiating event. The system function shall be maintained despite loss of Class IV power. The appropriate provisions shall be provided to ensure the reliability of isolation between HTS and LTC systems. The system shall satisfy the requirements of CNSC Regulatory Documents R-7 (Reference [4]) and R-9 (Reference [6]) The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006, 007.
34410	1(c), 1(d)	(Spent Fuel Bay) Cooling and Purification System	Maintain cooling of irradiated fuel during normal plant operation and accident conditions.	The cooling water inventory in the bay shall not drain during any events, including random pipe breaks in associated cooling systems and earthquake. The system shall provide makeup water to the spent fuel bay if the inventory is depleted via vaporization after a seismic event. Alternatively, it may be shown by providing another qualified water makeup source to SFB to make sure that the spent fuel can be cooled properly for a long term, during and after a seismic event. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 004, 005, 007.
34710	2(a)	Liquid Injection Shutdown System	See 68300	See 68300
34980	1(c)	Annulus Gas System	Monitor the integrity of the HTS pressure boundary (pressure tubes).	The system shall maintain suitable conditions in the annulus during normal plant conditions to ensure that deterioration of the pressure tubes does not occur. The system shall detect leakage of HTS coolant into the annulus during normal plant conditions to enable the operator to place the reactor in a safe condition.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
35000	FUEL HANDLING AND STORAGE			
35100	1(d)	New Fuel Transfer and Storage	Limit the release of radioactive material by maintaining the containment boundary.	The NF-Port, which is part of the NF Transfer system, shall maintain the containment envelope. During NF transfer, the NF-Port together with other NF transfer equipment and/or fuel changing equipment shall maintain the containment envelope. (see also ASI 35200) Appropriate provisions shall be provided to prevent fuel from criticality. The system shall satisfy the requirements of CNSC Regulatory Document R-7 (Reference [4]). The requirements of the following Safety Design Guides shall be satisfied: 69-03650-SDG–002, 003, 005, 006, 007.
35200	1(a), 1(d)	Fuel Changing	Maintain the integrity of the HTS pressure boundary. Provide fuel cooling during transfer to the fuel storage bay. Limit the release of radioactive material by maintaining the containment boundary.	During normal plant operation, the system shall remove decay heat from the fuel in the FM head while attached to the reactor, during transit to the spent fuel port, and while the fuel is being transferred to the storage bay. The radioactive release from the irradiated bundles inside the FM due to the loss of coolant supply shall not exceed the regulatory dose limits. The FM shall maintain the HTS pressure boundary, while attached to a fuel channel with the closure plug removed (i.e., remain attached to the tube). The fuel machine shall not damage (by striking) or overstress the HTS pressure boundary, whether or not the closure plug is removed. During NF or SF transfer, the NF Port or SF Port, together with other NF or SF transfer equipment and/or fuel changing equipment, shall maintain the containment envelope.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
				The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 005, 006, 007.
35300	1(c), 1(d)	Spent Fuel Transfer and Storage	Maintain the inventory in the irradiated fuel storage bay.	The cooling water inventory in the bay and transfer system shall not drain during any event, including random pipe breaks in associated cooling systems and earthquake.
			Provide fuel cooling during transfer to the fuel storage bay.	During normal operation, the system shall remove decay heat from the fuel in the Spent Fuel Transfer system while the fuel is being transferred to the storage bay.
			Limit the release of radioactive material by maintaining the containment boundary.	When the FM is not attached to the SF-Port, the SF-Port shall maintain the containment envelope. During SF transfer, the SF-Port together with other SF transfer equipment and/or fuel changing equipment, shall maintain the containment envelope. During SF transfer, radioactive release from fuel damage induced by a design basis event shall not exceed the regulatory dose limits and shall not cause fuel criticality. The requirements of the following Safety Design Guides shall be followed: 108-03650-SDG-002, 003, 006, 007.
35360	1(c), 1(d)	Storage Bay	Maintain cooling of irradiated fuel during normal plant operation and accident conditions.	Storage bay equipment shall be designed to prevent fuel from inadvertent criticality, and to protect fuel from damage so that the regulatory release limits are not exceeded. The requirements of the following Safety Design Guides shall be followed: 108-03650-SDG-002, 007.
35730	1(d)	FM Cable and Hose Management System	See 35200	See 35200

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
36000	STEAM GENERATOR SYSTEMS			
36100	1(c), 2(c)	Steam and Relief Systems	Remove heat from the HTS to provide fuel cooling.	For events in which adequate inventory can be maintained in the HTS, the SGs and MSSVs shall be capable of removing residual and decay heat immediately after shutdown, until other systems (FW from RWT, long term cooling, emergency core cooling become available to maintain effective longer term heat sinks. See 43230 and 34340 for FW supply requirements. The system shall provide overpressure protection for the steam generators. For a random steam line break or FW line break outside the reactor building, the main steam safety valves on the intact steam line shall continue to perform their heat removal function. Means to isolate each steam generator shall be provided in case of SGTR or MSLB. Suitable monitoring of leaking tubes and the level of radioactive materials in the secondary side shall be provided. The requirements of CNSC Regulatory Document R-7 (Reference [4]) shall be satisfied. The requirements of the following Safety Design Guides shall be followed: 108-03650-SDG-002, 003, 004, 005, 006
36310	1(d)	Steam Generator Blowdown System	Maintain the heat removal capability of the SGs	The system shall be designed to ensure that its failure will not cause loss of the SGs as a heat sink. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 006.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
37000	1(a)	FUEL	Maintain integrity of the fuel cladding in the core and maintain bundle integrity.	The fuel shall withstand anticipated operational transients and design basis events, and the cladding shall maintain its structural integrity, except for loss of coolant events where the coolant flow over the fuel is reduced to impair cooling. The new fuel storage and packaging areas shall be provided with fire protection and criticality protection. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 005, 007.
41600	1(d)	Oil Fire Protection System	Provide fire protection to prevent fires from spreading to safety related systems	The design of the system shall comply with the fire protection requirements outlined in Safety Design Guides 108-03650-SDG-005 and CAN/CSA N293.
43000	FEEDWATER AND AUXILIARY STEAM SYSTEMS			
43230	1(c), 2(c)	Feedwater System (includes Auxiliary Feedwater, Deaerator and Deaerator Storage Tank)	Maintain heat removal capability from the HTS to provide fuel cooling.	The system shall provide AFW to the SGs to remove residual and decay heat after reactor shutdown, in conjunction with the inventory contained in the SG. The system shall provide AFW to the SGs for pressures ranging from the design setpoint of the MSSVs to their fully open condition. The system shall provide AFW automatically on loss of Class IV power or loss of the main FW system. The system shall be designed to ensure that its failure will not cause loss of the SGs as a heat sink at a frequency exceeding that permitted by the PSA. Instrumentation and control required to maintain automatic Steam Generator Level Control (SGLC) during and for at least 30 minutes following a LOCA or MSLB shall be environmental qualified to ensure the SG heat sink capability. The requirements of CNSC Regulatory Document R-7 (Reference [4]) shall be satisfied.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
				The requirements of the following Safety Design Guides shall be followed: 108-03650-SDG-002, 003, 004, 005, 006.
50000	ELECTRIC POWER SYSTEMS			
50000	1(c), 2(c)	Electric Power System	Provide electrical power to enable safety related systems to perform their safety functions during normal operation and following an event, as required.	The system shall provide electrical power to all safety related systems during normal station operation and following an event. To satisfy reliability requirements to meet safety objectives, the system shall be equipped with standby diesel generators and designed to ensure that its failure will not cause loss of safety function of mitigating systems required to be supported at a frequency exceeding that permitted by the PSA. Failure of the system due to the random failure of components shall be minimized through the use of redundant components. The requirements of CNSC Regulatory Document R-7 (Reference [4]) and R-9 (Reference [6]) for support services for Safety Systems, and S-98 (Reference [3]) shall be satisfied. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006.
52000	2(c)	Standby Generators	Maintain the electrical power generating capacity as needed by the safety related systems.	See 53000 Distribution System.
53000	1(c), 2(c)	Distribution System	Provide electrical power to enable systems to perform their safety functions as required.	The power distribution system shall be designed to prevent propagation of electrical faults between the redundant ODD and EVEN divisions. Provision to provide seismically qualified electrical power supply shall be incorporated in the design for components operating during or following a seismic event.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
				The requirements of CNSC Regulatory Document R-7 (Clause 2.2(b)) (Reference [4]) and R-9 (Clause 2.2) (Reference [6]) for support services for Safety Systems and S-98 [3] shall be satisfied. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006.
56000	1(d)	Lighting and Building Service Systems	Maintain lighting and other services to enable operating staff to perform monitoring and control functions for safety related systems.	The system shall provide lighting and any required building services in the MCR, the SCA, the route for access to the SCA, and any associated control areas, during events for which these control areas are required to remain available. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 004, 005.
57000	1(c), 2(c)	Cabling System	Maintain power supply to enable safety related systems to perform their safety functions as required.	The system shall provide an electrical power supply to safety related systems, during events for which these systems are required to remain available. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005.
57600	2(b)	(Electrical) Containment Penetrations	Maintain barrier to the release of radioactive material.	The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006.
60000	INSTRUMENTATION AND CONTROL			
61500		Seismic Instrumentation Equipment	Monitor seismic activities.	See Specific system The requirements of the following Safety Design Guide shall be satisfied: 108-03650-SDG-002.
63000	REACTOR, REACTOR SYSTEMS AND AUXILIARIES INSTRUMENTATION			
63101 63102	1(c)	Channel Flow Measurement Channel Temperature Monitoring	Monitor the coolant flow and temperature to confirm adequate fuel cooling during normal plant operation.	The system shall be capable of detecting fuel channel blockage that could lead to fuel failure or reduced safety margin due to overheating. The requirements of the following Safety Design Guide shall be satisfied: 108-03650-SDG-002.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
63103	1(c)	Gaseous Fission Product Monitoring	Continuously monitor on-power, the integrity of the fuel in the reactor.	The system shall be capable of detecting defective fuel in the reactor during normal plant operation at power.
			Maintain the integrity of the HTS during a seismic event.	The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 007.
63108	1(c)	Failed Fuel Detection (System)	Locate small fuel defects while reactor is at power.	The system shall be capable of locating small fuel defects in the reactor while it is at power during normal plant operation.
			Maintain the integrity of the HTS during a seismic event.	The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 007.
63700	1(c), 1(d)	Plant Control	Provide control and monitoring of safety related systems during normal plant operation.	The system shall provide control and monitoring capability in the MCR for normal operation and for all events for which the MCR remains available.
			Control the reactor within specified conditions during normal operation to prevent loss of regulation incidents.	Control includes all reactivity control units, including zone control units.
			Shut down the reactor for events anticipated to occur frequently during plant life.	During accident conditions, the system shall fail in a manner that does not put the plant (e.g., reactor control, pressure and inventory control, SG pressure and level control) in a state exceeding the shutdown capability of SDS1 or SDS2. This may require environmental or seismic qualification of certain components, depending on their specific failure characteristics. (Also see 68200, 68300)
				The requirements of CSA N290.4 (Reference [7]) shall be satisfied.
				The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 004, 005.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
66000	1(c), 2(c)	CONTROL CENTRE	Provide control and monitoring during normal operation and after all accident conditions for which the control room remains available and habitable.	The control centre and MCR shall be designed to enable the operator to perform monitoring and control functions for normal operation and accident conditions, except those events for which the control room becomes unavailable. The control centre and MCR shall be designed to be operable following an earthquake, a fire outside the MCR, or loss of Class IV electrical power, and the operator must remain available to proceed to the SCA. The MCR shall be designed to be protected from flooding. Connections to the SCA shall be buffered so failures in the SCA will not interfere with control and monitoring during normal and accident plant conditions. The requirements for monitoring and control of the Safety Systems and associated support systems specified in the CNSC Regulatory Documents R-7 (Reference [4]), R-8 (Reference [8]), and R-9 (Reference [6]) shall be satisfied. The requirements for post-accident monitoring specified in CSA Standard N290.6 (Reference [9]) shall be satisfied. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 007.
66600	2(c)	Secondary Control Area	Provide the capability to shutdown the reactor and maintain it in a safe shutdown state, and monitor the plant under accident conditions.	The SCA shall remain available to carry out monitoring and control functions for abnormal plant operating conditions, including those in which the MCR becomes unavailable. Actions in one control room shall not prevent the operators from placing the plant in safe shutdown state from the other control room. The requirements for monitoring and control of the Safety Systems and associated support systems specified in the CNSC Regulatory Documents R-7 (Reference [4]), R-8 (Reference [8]), and R-9 (Reference [6]) shall be satisfied.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
				The requirements for post-accident monitoring specified in CSA Standard N290.6 (Reference [9]) shall be satisfied. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 007.
67000	COMMON PROCESSES AND SERVICES			
67147	1(d)	Fire Detection and Alarm System	Provide the capability to detect fires that could potentially damage safety related systems.	The requirements specified in CSA Standard N293 (Reference [10]) shall be satisfied. The following Safety Design Guide shall be satisfied: 108-03650-SDG-005.
67314	2(b)	Containment Isolation	Establish the containment barrier for normally open pathways from the HTS or containment atmosphere to the environment.	The system shall automatically close normally open pathways through the containment envelope for events that would otherwise cause the regulatory dose limits for the public to be exceeded. The system shall, as a minimum, perform its function on pressures or radiation levels that indicate a loss of coolant accident or fuel failures requiring an intact containment envelope. The requirements of CNSC Regulatory Document R-7 (Reference [4]) shall be satisfied. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006
68000		SAFETY SYSTEMS		
68200	2(a)	Shutdown System No. 1 (SDS1)	Shut the reactor down and maintain it in a safe shutdown condition.	The requirements of CNSC Regulatory Documents R-8 (Reference [8]) and R-10 (Reference [11]) shall be satisfied.
68300		Shutdown System No. 2 (SDS2)		The requirements of CSA Standard CAN3-N290.1 (Reference [12]) shall be satisfied. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
68400	2(b)	Containment System (see 67314 for Containment Isolation System)	Barrier to the release of radioactive materials within the containment envelope. (Also see 21000, 67314, 73140).	The containment system shall provide a barrier against the release of radioactive materials beyond normal operational levels, which could cause regulatory dose limits for the public to be exceeded. The barrier shall be established using a combination of structures, isolation devices, and metallic extensions of the containment envelope (see Table 3). The requirements of CNSC Regulatory Document R-7 (Reference [4]) shall be satisfied. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006.
68440	2(b)	Containment Ventilation Isolation System	Establish the containment barrier for normally open ventilation ducts.	The system shall automatically close normally open ventilation ducts through the containment envelope for events which would otherwise cause the regulatory dose limits for the public to be exceeded. The system shall, as a minimum, perform its function on pressures or radiation levels which indicate a LOCA or fuel failures requiring a containment envelope. The requirements of CNSC Regulatory Document R-7 (Reference [4]) shall be satisfied. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006, 007.
68480	1(d), 2(c)	Hydrogen Control System	Maintain the integrity of the containment envelope and safety related systems.	Provisions shall be made for controlling the concentration of hydrogen and/or oxygen following an accident to prevent explosion or deflagration, by providing ignition of flammable concentrations in local areas, or by other means. The system shall satisfy the requirements of CNSC Regulatory Document R-7 (Reference [4]). The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
68570	2(b)	Second Crash Cooldown System	Depressurize the secondary side of the SGs to assist the fuel cooling function.	The system shall open a sufficient number of MSSVs to depressurize the HTS to assist the ECC, moderator systems in cooling the fuel, or to introduce an alternate water source from the RWS to the SGs, when required. The system shall satisfy the requirements of CNSC Regulatory Documents R-9 (Reference [6]). The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006.
68900	2(c)	Post Accident Management	Maintain the integrity of the containment envelope and safety related systems	The requirements for post-accident monitoring specified in CSA Standard N290.6 (Reference [9]) shall be satisfied. Post-accident monitoring EQ and SQ requirements on instrumentation of systems shall be identified. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004.
70000	COMMON PROCESSES AND SERVICES			
71000	WATER SYSTEMS			
71310 71340	1(c), 1(d), 2(c)	Raw Service Water system Recirculated Cooling Water system	Provide cooling water to safety related systems to prevent the occurrence of accident conditions, and to mitigate the effects of accident conditions.	The systems shall provide cooling water, as required, to safety related systems to maintain normal plant conditions. For any service water load shedding after loss of Class IV, failure mode of load shedding devices under harsh conditions created by an accident shall be considered to ensure the system proper operation.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
				The systems shall provide cooling water to the following safety related systems as applicable for mitigation of accident conditions: • LTC system, • LACs, • Standby DGs, • Instrument air compressor; • FW pumps, • Moderator system, and • Shield cooling system The systems shall have reliability as established in PSA. The systems shall satisfy the requirements for emergency core cooling and containment support systems imposed by R-7 (including clause 2.2(b) (Reference [4]) and Appendix) and R-9 (Reference [6]). Provision to provide seismically qualified supply to the safety related systems shall be incorporated. (see 108-03650-SDG-002). The systems shall satisfy the requirements of the following Safety Design Guides: 108-03650-SDG-002, 003, 004, 005, 006.
71400	1(d)	Fire Water Protection System (Fire Water Supply System)	The Fire Protection System provides fire protection to prevent fires from spreading to safety related systems. Provide a fire water supply to the fire protection system.	The system shall satisfy the requirements of the following Safety Design Guides: 108-03650-SDG-002, 004, 005, 006. The requirements of CAN/CSA N293 (Reference [10]) shall be satisfied.
71900	1(d)	Chilled Water System	Provide acceptable environmental conditions for safety related systems.	Provide seismically qualified supply to the chilled water loads operating during or following a seismic event. The requirements of the following Safety Design Guides shall be satisfied: 98-03650-SDG-002, 006.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
72200		Fuel Oil Systems	Provide fuel for standby and emergency generators	See 50000
73000	HEATING, COOLING AND VENTILATION SYSTEMS			
73110	1(d), 2(c)	(Reactor Building) Cooling System	Provide cooling to the RB during plant normal operation. Provide cooling of the RB during and following a LOCA or MSLB in the RB. Continue circulating the air in RB after a LOCA and following a SDE to prevent build-ups of hydrogen concentration. Provide acceptable environmental conditions for safety related systems.	The cooling system shall maintain RB inside temperature below the maximum allowable during normal operating conditions. During and following a LOCA or MSLB the local air coolers shall remain functional to remove heat from the RB atmosphere to reduce the RB atmosphere temperature and pressure to normal conditions. The RB cooling system shall assist in dispersal of hydrogen following a LOCA and continue this function after an SDE which may occur 24 hours after a LOCA. The system shall satisfy the requirements imposed by CNSC Regulatory Document R-7. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006
73120	1(c), 1(d)	(Reactor Building) Ventilation System	Provide acceptable environmental conditions for safety related systems	The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006, 007.
73140	2(b)	Reactor Building Containment Isolation	See 68400	see 68400, 67314
73350 73360	1(d)	RSW Pumphouse Heating System RSW Pumphouse Ventilation System	Provide acceptable environmental conditions for safety related systems.	The systems shall provide heating or cooling, as required, to maintain the safety functions of safety related systems during events requiring those functions, and during the normal operation of the plant as required to achieve their intended design life. (See 71000) The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 004, 005.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
73410 73420	1(d), 2(c)	(RAB) Heating System (RAB) Ventilation System	Provide acceptable environmental conditions for safety related systems.	The systems shall provide heating or cooling, as required, to maintain the safety functions of safety related systems during events requiring those functions, and during the normal operation of the plant as required to achieve their intended design life. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 004, 005.
73510	1(d), 2(c)	Main Control Building (HVAC)	Provide cooling to safety related control and display components.	The system shall provide cooling, as required, to maintain the functions of safety related control and display systems in the MCR for all events except the MCR uninhabitable. The system shall satisfy the requirements of the following Safety Design Guides: 108-03650-SDG-002, 004, 005.
73520	2(c)	Secondary Control Area (HVAC)	Provide cooling to safety related control and/or display components.	The System shall provide cooling, as required, to maintain the functions of safety related systems. The system shall satisfy the requirements of the following Safety Design Guides: 108-03650-SDG-002, 004, 005.
73900	1(d), 2(c)	Miscellaneous Structures (HVAC)	Provide cooling to protect safety related systems.	The system shall provide heating or cooling, as required, to maintain the functions of safety related systems. The system shall satisfy the requirements of the following Safety Design Guides: 108-03650-SDG-002, 004, 005.
75000		COMPRESSED GASES		
75120	1(d), 2(c)	Instrument Air	Provide instrument air to safety related systems to prevent the occurrence of accident conditions and to mitigate the effects of accident conditions.	The system shall provide instrument air, as required, to safety related systems to maintain normal plant conditions. The system shall be designed so the instrument air supply to systems inside containment can be isolated after release of radioactive material inside the containment envelope, if required to remain within the containment design pressure, or to satisfy regulatory dose limits.

ASI	Safety Category	System or Structure	Safety Function	Safety Requirements
				Alternate sources of instrument air such as local air tanks shall be provided for safety related systems that are required to perform safety functions following an earthquake or other event which could cause the failure of the normally operating system. (see 108-03650-SDG-004). The requirements of CNSC Regulatory Documents R-7 (Reference [4]), R-8 (Reference [8]) and R-9 (Reference [6]) shall be satisfied. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-002, 003, 004, 005, 006.
75600	1(d)	Combustible Gases	Prevent damage to safety related systems during a failure which causes a fire.	The system shall be located so that the requirements of the Fire Protection Program are satisfied. The requirements of the following Safety Design Guides shall be satisfied: 108-03650-SDG-005.
76000	1(d)	Material Handling (Cranes and Hoists)	Maintain structural integrity to prevent damage to safety related systems	Cranes and hoists shall be located so their failure during an earthquake will not damage seismically qualified components, or else they shall be qualified to withstand the earthquake. The following Safety Design Guide shall be satisfied: 108-03650-SDG-002.
78000		MISCELLANEOUS SYSTEMS AND EQUIPMENT		
78200		Fuel Oil Systems	See specific user system	See specific user system
79000	1(d)	RADIOACTIVE WASTE MANAGEMENT	Ensure that regulatory dose limits are not exceeded for design basis events, including earthquakes.	The following Safety Design Guide shall be satisfied: 108-03650-SDG-002, 005, 006, 007.

Table 3
Systems/Components Forming Part of the Containment Boundary

The systems listed below shall satisfy the requirements for metal extensions of the containment envelope as described in 108-03650-SDG-006 and CNSC Regulatory Document R-7 (Reference [4]) for the portion of the system which passes through the containment envelope.

ASI	System
21600	Special Equipment (Airlocks, Shielding Doors, Blowout Panels, Atmosphere Barriers, Equipment Hatch)
32300	Moderator Cover Gas System
32500	(Moderator) Heavy Water Collection Systems
32600	(Moderator) Heavy Water Sampling Systems
33530	HT Nitrogen Addition System
33540	HT Hydrogen Addition System
33710	HT Sampling System
33810	HT Collection System
34320	Emergency Coolant Injection System
34350	Long–Term Cooling System
34510	Resin Transfer System
35100	New Fuel Transfer and Storage
35200	Fuel Changing
35300	Spent Fuel Transfer and Storage
36100	Steam and Relief Systems
36310	Steam Generator Blowdown System
36400	Controlled Steam Discharge Systems - Blowoff
36600	Steam Generator Water Sampling System
38100	Heavy Water Supply System
38310	Heavy Water Vapour Recovery System
43230	Feedwater System
57600	(Electrical) Containment Penetrations
63862	Heavy Water in Light Water (Leak Detection)
67314	Containment Isolation
67857	Radiation Protection Equipment
68200	Shutdown System No. 1 (SDS1)
68300	Shutdown System No. 2 (SDS2)
68400	Containment System (see 67314 for Containment Isolation System)
68440	Containment Ventilation Isolation System
68480	Hydrogen Control System
71340	Recirculated Water System
71400	Fire Water Protection System (Fire Water Supply System)

ASI	System
71650	Demineralized Water System
71730	Active Drainage Reactor Building
71900	Chilled Water System
73110	(Reactor Building) Cooling System
73120	(Reactor Building) Ventilation System
73140	Containment Isolation
75110	Plant Service Air
75120	Instrument Air
75130	Breathing Air
75300	Hydrogen Circuit
75500	Oxygen System (for moderator cover gas)
75700	Nitrogen (System)
79140	Solid Waste Spent Resin Management System
79310	(Gaseous Wastes) Discharge System
79320	Offgas Waste Management System

Table 4
Systems and Structures Considered in Radiation Protection

The design of the systems or structures listed below shall be considered in the Radiation Exposure Control Program. The principal radiation hazards from the process systems and components are described in 108-03650-SDG-007.

ASI	System
21600	Special Equipment (Airlocks, Shielding Doors, Blowout Panels, Atmosphere Barriers, Equipment Hatch)
24250	Spent Fuel Bay
30100	Nuclear Safeguard System and Equipment
30700	Special and Consumable Materials
30800	Process Systems Components
30900	Miscellaneous Components For Nuclear Process Systems
31000	Reactor
31700	Reactivity Control Units
31800	Reactor Shielding
31900	Installation and Maintenance Equipment
32100	Moderator Systems
32200	(Moderator) Purification System
32300	(Moderator) Cover Gas System
32500	(Moderator) Heavy Water Collection Systems
32600	(Moderator) Heavy Water Sampling Systems
32700	(Moderator) Liquid Poison Systems
33100	Heat Transport System
33310	Heat Transport Pressure and Inventory Control System
33340	Heat Transport Pump Seal System
33350	Heat Transport Purification System
33710	Heat Transport Sampling System
33810	Heat Transport Water Collection System
34110	Shield Cooling System
34320	Emergency Coolant Injection System
34350	Long-Term Cooling System
34410	(Spent Fuel Bay) Cooling and Purification System
34510	Resin Transfer System
34710	Liquid Injection Shutdown System
34980	Annulus Gas System
35100	New Fuel Transfer and Storage
35200	Fuel Changing

ASI	System
35300	Spent Fuel Transfer and Storage
35510	Fuel Channel Component Handling Tools
37000	Fuel
38100	Water Supply System
38310	Heavy Water Vapour Recovery System
38910	Miscellaneous Heavy Water Collection
38920	Heavy Water Sorting Station
38930	Drum Cleaning Facilities
61300	Radiation Monitoring and Sampling Equipment
63103	Gaseous Fission Product Monitoring
63108	Failed Fuel Detection (System)
68440	Containment Ventilation Isolation System (Also see 73120)
71730	Active Drainage Reactor Building
71740	Active Drainage Reactor Auxiliary Building and Services Building
73120	(Reactor Building) Ventilation System
73440	Decontamination Centre Ventilation
73470	Spent Fuel Bay Ventilation System
79100	Solid Wastes
79140	Spent Waste Resin Management System
79210	Liquid Waste Management System
79310	(Gaseous Wastes) Discharge System
79320	Offgas Waste Management System

Appendix A

Major Systems' Safety Functions

A.1 Reactor Shutdown

The reactor can be shut down by either dedicated Shutdown Systems (SDS1 and SDS2) for design basis events, or by the Reactor Regulation System (RRS) during normal plant operations and anticipated transient conditions.

A.1.1 Shutdown Systems

The reactor will be shut down by two fast acting, fully capable, diverse and independent shutdown systems, one based on absorber rods (SDS1) and the other based on injection of soluble poison (SDS2). Both SDS1 and SDS2 will be capable of independently and automatically shutting the reactor down if abnormal conditions are detected. For events requiring prompt shutdown action, each shutdown system shall be designed such that, acting alone, it can ensure that:

- the reactor is rendered subcritical and is maintained subcritical;
- the reference dose limits are not exceeded, and
- a loss of primary heat transport system integrity will not result from any fuel failure mechanism.

A.1.2 Reactor Regulation System

The Reactor Regulation System (RRS) will be capable of shutting the reactor down or reducing reactor power either manually or automatically for normal operation or anticipated operational occurrences.

A.2 Heat Removal from the Fuel

The heat sink systems that are considered to be safety related are those that remove the stored and decay heat following reactor shutdown. During normal plant operation, heat is removed from the fuel by the steam system, or by the long term cooling system. Refer to Figure A-1 for a schematic representation of the pathways for the transfer of heat from the fuel in the reactor to an ultimate heat sink.

For accident conditions or external events, heat is removed from the fuel by the steam system, by the two sub-systems of the ECC system, the ECI and LTC. If the ECC system fails, the fuel will heat up and a set of voided pressure tubes will sag into their calandria tubes. At this stage, the heat removal path is relied on the large moderator heat sink. Fuel melting will not take place at decay heat level provided heat can be removed through the moderator cooling system. However, if the moderator system is unavailable, the accident is progressed into the SCDA, and the defence is the shielding tank. The calandria vessel holding the moderator is itself surrounded by a water-filled shielding tank, which acts as a further passive heat sink, to delay the SCDA progression.

The operation of the above systems in performing their safety functions is described in more detail below.

A.2.1 Steam System

The steam system removes heat to cool the reactor during normal or accident conditions. The major components that perform the heat removal function are the SGs, the FW supplies, and the MSSVs.

For normal plant conditions, FW is supplied from the main FW system using the FW pumps following a reactor shutdown. When the Class IV power is lost, FW is supplied using AFW pumps. The main FW system supplies water to the SGs to maintain their required levels for heat removal. The auxiliary feed pumps are sufficient to remove stored and decay heat, in conjunction with the stored inventory in the SGs at the time of reactor shutdown. Although the main FW pumps may also be available (if Class IV power remains available), they are not credited with a safety related function and are not designated as being safety related.

For accident conditions, the FW system is backed up by the reserve water system. If the FW system fails, the RWS provides an independent supply of FW by gravity to the SGs, with an inventory suitable until an alternative heat sink can be established.

The MSSVs are used to reject the heat to the ultimate heat sink, which in this case is the atmosphere. These are spring loaded relief valves that also protect the steam system from overpressure, in addition to their heat rejection function. For their heat rejection functions, they are equipped with actuators which manually or automatically open the MSSVs to depressurize the steam generators in response to a design basis event for maximum heat removal rate. This depressurization allows FW to be supplied at low pressure after initial heat removal, and also rapidly cools and depressurises the HTS to assist the ECI or moderator systems in cooling the fuel.

A.2.2 Emergency Core Cooling System (ECCS)

In a LOCA, the ECC system refills the fuel channels and removes decay heat from the reactor fuel. This is accomplished by means of a high-pressure injection phase (ECI) and a low pressure pumped recovery phase (LTC). The initiation of the ECI system is automatic on a LOCA signal, which also initiates crash cooldown of the SG by opening the MSSVs to assist rapid depressurization of the HTS. The ECI system is also capable of making up for shrinkage due to rapid cooling (e.g., MSLB event) with an intact pressure boundary.

The LTC system provides both normal plant shutdown cooling as well as long term cooling after a LOCA. The LTC pumps and heat exchangers are cooled by Division 1[1] and Division 2 of the RCW system.

[1] Divisions are redundant sets of components within a given safety related system that are physically and functionally independent from each other for performing the essential safety functions.

A.2.3 Moderator

The low-pressure moderator removes heat from the reactor in normal operation (i.e. neutron moderation) through its own cooling system. Following an accident, heat removal is performed by the ECC system. However, if the ECC is unavailable, the moderator system serves as a back up heat sink to remove the fuel heat and maintains fuel channel integrity by providing pumped flow through the calandria. In addition, the RWS provides a passive water make-up supply to the moderator when required.

A.2.4 Shield Cooling System

The shield cooling system removes heat accumulated from the reactor structure by circulating cooling water through the end shields and shield tank such that the calandria is maintained at an appropriate stress level. The water-filled shielding tank serves the dual function of protecting radiological hazard from the worker during normal operation and as a passive emergency heat sink during a SCDA. In an event of triple failures (LOCA + LOECC + loss of moderator cooling), the shield tank is used to establish a passive heat sink. The shield tank inventory can be made up by the RWS to delay the accident progression.

A.2.5 Reserve Water System

The RWS provides make-up water to the SGs after depressurization when FW system is unavailable. It also dumps water to the RB sumps following a LOCA to establish long term cooling. For LCDA, the RWS provides make-up water to the HTS as a short-term heat sink, and the moderator for long term heat removal. For SCDA (i.e. LOCA+LOECC + loss of moderator cooling), the RWS provides make-up water to the moderator, and/or the shield tank as required.

A.2.6 Containment Cooling

For containment cooling, qualified LACs will gradually reduce the high pressure/temperature /humidity inside the RB after a LOCA or MSLB and continue long term cooling. Cooling water for the LACs is provided from RCW Divisions 1 and 2.

A.2.7 Recirculated Cooling Water and Raw Service Water

The two Divisions 1 and 2 of the RSW system are once-through systems that draw water from the ultimate heat sink[2] and use it to cool the RCW system, that in turn cools various safety related and non-safety related loads in the plant. The heat absorbed by the RSW is then transferred to the ultimate heat sink.

The RCW Division 1 and 2 are closed loop systems whose function is to provide cooling water to equipment across the plant including both safety related loads. These loads include heat exchangers, air coolers, pumps and pump motors. The heat absorbed by the RCW system is then rejected to the RSW systems via heat exchangers. The Division 1 RCW system removes heat from the designated Division 1 systems and equipment, and the Division 2 RCW removes heat from the designated Division 2 systems and equipment, but each can back up the other through

[2] The ultimate heat sink may be a large body of water such as a lake, river or ocean, or the atmosphere via cooling towers.

an interconnection where redundant cooling water supplies are needed for reliability reasons. This concept also applies to the RSW systems.

A.3 Containment Systems

During normal plant operation, radioactive materials are contained within the boundaries of various systems and structures designed for this purpose (e.g., fuel element, heat transport system, spent fuel bay).

In a design basis event where these normal boundaries are damaged, the Containment system provides a barrier against the release of radioactive materials that could cause regulatory dose limits for the public to be exceeded. Containment isolation occurs automatically when high activity or an abnormally high pressure is detected in the RB. A continuous containment envelope is established using a combination of structures, isolation devices, and metallic extensions of the containment envelope. Containment cooling features may be provided to limit the peak temperature and pressure that could occur within the containment envelope, and to reduce the temperature and pressure in the long term.

For hydrogen control in containment after an accident, a hydrogen control system uses passive hydrogen recombiners to limit the concentration of hydrogen or deuterium gas within containment.

A.4 Monitoring and Control Systems

All events, including the seismic event, will be handled from the MCR. Only events causing MCR uninhabitability (e.g. fires, hostile takeover, etc.) will be handled from the SCA to shutdown the reactor and maintain it in a safe shutdown state, and monitor the plant states. Post accident management (PAM) has the following functions:

- Provide the plant operator with information to monitor post accident conditions and systems in the plant.
- Provide the plant operator with appropriate control mechanisms to be able to control the post accident situation.

In practice, PAM is not a completely independent system. It makes maximum use of other qualified instrument loops and equipment designed as part of the normal power production and safety related systems, but will provide additional equipment or measurement loops if necessary. All PAM information will be clearly and uniquely distinguishable from that provided by other systems.

A.5 Support Services

The major support services for the safety related systems include the cooling water systems (described above with heat sinks), the electrical system, the compressed air systems, and the ventilation systems.

A.5.1 Electrical System

The ODD and EVEN power supplies provide interchangeable electrical energy to power production related equipment and safety related systems. The electrical system is composed of four classes of power supplies:

- Class IV is AC power which is available from the grid or the turbine generator,
- Class III is qualified AC power supplied from Class IV but is backed up by dedicated standby diesel generators which are seismically qualified,
- Class II is a stored energy, seismically qualified, highly reliable AC power supply and is a constituent part of Uninterruptible Power Supply (UPS) and
- Class I power is a stored energy, seismically qualified, highly reliable DC power source and is a constituent part of UPS.

The Class I, II, and III electrical power supplies that supply power to safety related loads are considered to be safety related. Any connected load or supply that is not safety related can be reliably isolated to minimize the unavailability of the safety related supply.

Although the Class IV supply from the grid to Class III is not designated as safety related, it is designed to be re-established as soon as possible after a design basis event.

A.5.2 Instrument Air Systems

The nuclear steam plant receives compressed air (instrument air, service air and breathing air) from the compressed air system during normal plant operation. For a design basis event, a backup supply (e.g., local air tanks) is provided to supply instrument air to essential users during a loss of the normal air supply.

A.5.3 Ventilation Systems

The ventilation systems provide a suitable operating environment for safety related systems during normal operation. During accident conditions, reliance on ventilation systems (including air conditioning) is minimized, but still needed for areas like the control rooms and control equipment rooms, where heat generated by the systems that are required to operate must be removed.

During normal operation and design basis events that do not involve a release of radioactive material in the reactor building, the reactor building ventilation system provides air exchange for habitability and cooling, maintains the reactor building at a pressure slightly below atmospheric to minimize release of radio-nuclides to the environment, provides filtration of air before exhaust to the atmosphere. During accident conditions involving a release of radioactive material in the reactor building, the ventilation system is not credited as it may be isolated to establish the containment envelope.

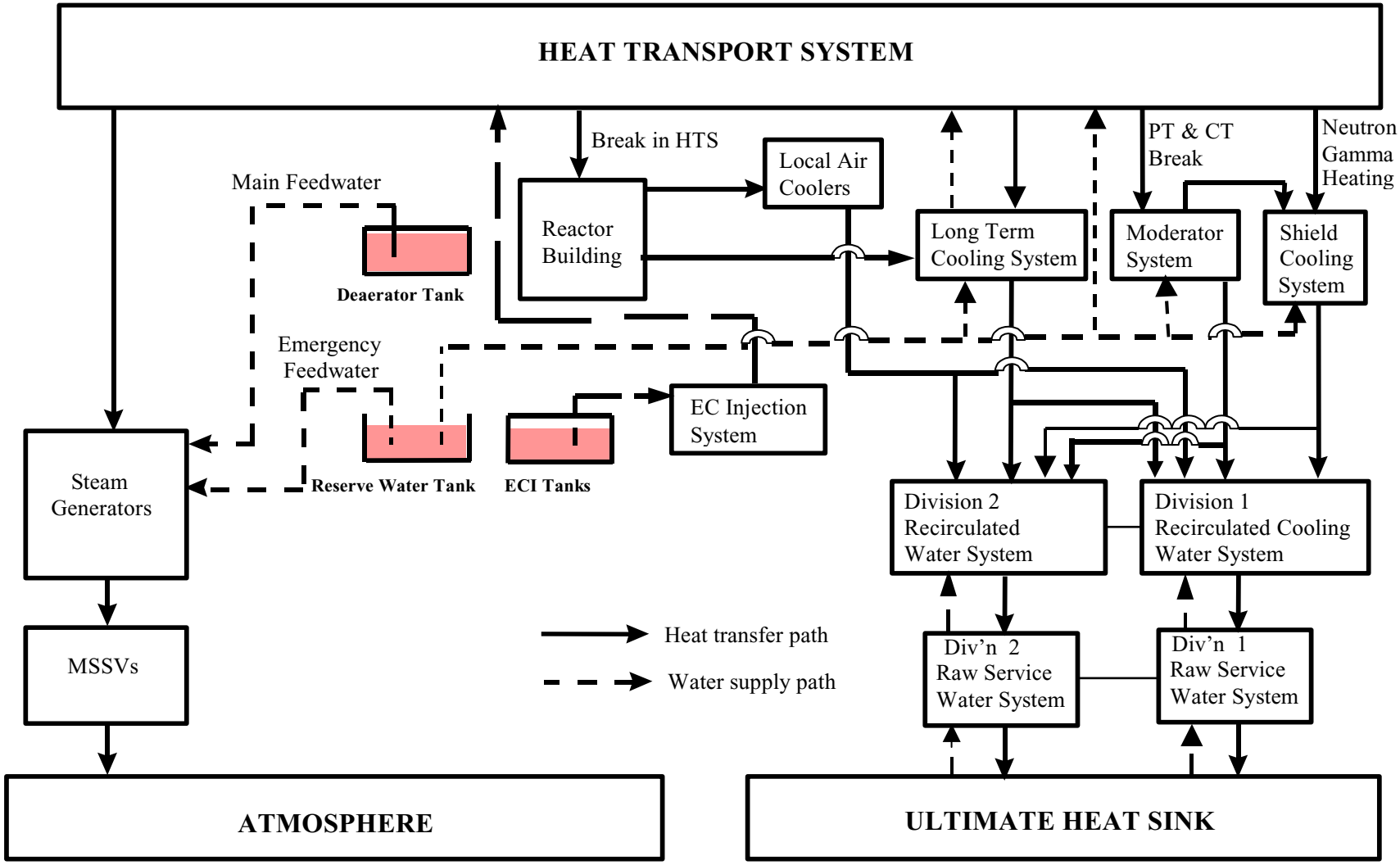

Figure A-1 Schematic of Safety Related Systems Which Transfer Residual Heat to the Ultimate Heat Sinks

Appendix B

List of Safety Design Guides

Identification	Title
108-03650-SDG-001	Safety Related Systems
108-03650-SDG-002	Seismic Requirements
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 C

Acronyms

3D CAD	Three Dimensional Computer Aided Design
AC	Alternating Current
ACR	Advanced CANDU Reactor
AECL	Atomic Energy of Canada Limited
AFW	Auxiliary Feedwater
ALARA	As Low As Reasonably Achievable
ASDV	Atmospheric Steam Discharge Valves
BOP	Balance Of Plant
CA	Control Absorber
CAE	Computer Aided Engineering
CAMLS	CANDU Alarm Message List System
CANDU	CANadian Deuterium Uranium
CBM	Condition Based Maintenance
CCP	Critical Channel Power
CCW	Condenser Cooling Water
CED	Contract Effective Date
ChemAND	Chemistry ANalysis and Diagnostic system
CHF	Critical Heat Flux
CNSC	Canadian Nuclear Safety Commission
COG	CANDU Owners Group
CRT	Cathode Ray Tube
CSA	The Canadian Standards Association
D_2O	Heavy Water
DBE	Design Basis Earthquake
DC	Direct Current
DCS	Distributed Control System
DE	Design Basis Accident
DEL	Derived Emission Limit
DG	Diesel Generator
DUPIC	Direct Use of spent PWR fuel In CANDU
EAB	Exclusion Area Boundary
ECCS	Emergency Core Cooling System
ECI	Emergency Coolant Injection
EDS	Electrical power Distribution System
EQ	Environmental Qualification
FM	Fuelling Machine
FMEA	Failure Mode and Effect Analysis
HTS	Heat Transport System
HV	High Voltage
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
LV	Low Voltage
LWR	Light Water Reactor
MCR	Main Control Room
MOT	Main Output Transformer
MOX	Mixed Uranium and Plutonium Oxide Fuel
MSIV	Main Steam Isolation Valve
MSLB	Main Steam Line Break
MSSV	Main Steam Safety Valve
MSIV	Main Steam Isolation Valve
NEW	Nuclear Energy Worker
NF	New Fuel
NPSH	Net Positive Suction Head
NSP	Nuclear Steam Plant
NSR	Not Safety Related
OM&A	Operation, Maintenance and Administration
PAM	Post Accident Monitoring
PLEx	Plant Life Extension
PLiM	Plant Life Management
PT	Pressure Tube
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
RRS	Reactor Regulation System
RSW	Raw Service Water
RWS	Reserve Water System
RWT	Reserve Water Tank
SSMC	Safety System Monitor Computers
SCA	Secondary Control Area
SDE	Site Design Earthquake
SDG	Safety Design Guide
SDS 1	Shut Down System 1
SDS 2	Shut Down System 2
SEU	Slightly Enriched Uranium
SF	Spent Fuel
SFB	Spent Fuel Bay
SFC	Single Failure Criterion
SGLC	Steam Generator Level Control
SGTR	Steam Generator Tube Rupture
SQ	Seismic Qualification

SST	System Service Transformer
SU	Shutoff Unit
TB	Turbine Building
ULC	Underwriter's Laboratories Canada
UPS	Uninterrupted Power Supply
UST	Unit Service Transformer
ZCU	Zone Control Unit