AECL EACL

Licensing Submission

Classification of Safety Related Systems and Structures

ACR US

108US-03621-LS-001
Revision 0

Prepared by
Rédigé par

A. H. Stretch
Reactor, Safety, and Licensing Resources

Reviewed by
Examiné par

H. Johal
Reactor, Safety, and Licensing Resources

Approved by
Approuvé par

V. Langman, Manager
ACR US Licensing

2003 April

CONTROLLED - Licensing

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

Avril 2003

CONTRÔLÉ - Permis

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

AECL EACL

Licensing Submission

Classification of Safety Related Systems and Structures

ACR US

108US-03621-LS-001
Revision 0

2003 April

CONTROLLED - Licensing

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

Avril 2003

CONTRÔLÉ - Permis

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
Classification of Safety Related Systems and Structures	

CONTROLLED – Licensing / CONTRÔLÉ - Permis

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		D1	2003-04-16	Issued for Review and Comment.	A. H. Stretch	H. Johal W. Rabbani K. Hau M. Bonechi C. Reid (Bechtel)	V. Langman
2		0	2003-04-30	Issued as “Approved for Use”.	A. H. Stretch	H. Johal	V. Langman

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°
	108US	03621	LS	001	1	1	

TABLE OF CONTENTS

1. PURPOSE

AECL will be applying to the US NRC for the Design Certification of the Advanced CANDU® Reactor™ (ACR™*) design. This document provides information about the generic design of the ACR to the US NRC as part of the pre-application activities. This document outlines the method of identifying and classifying safety related structures and systems for the ACR design, which is applied to the design through Safety Design Guide 108-03650-SDG-001 “Safety Related Systems” (Reference [2]).

® CANDU (CANada Deuterium Uranium) is a registered trademark of Atomic Energy of Canada Limited (AECL).

* ACR™ (Advanced CANDU Reactor™) is a registered trademark of AECL.

2. OBJECTIVES

The objective of this report is to provide:

1. the definition of safety related systems for the ACR design,
2. the classification of safety related systems used for the ACR, and
3. a list of the safety related systems that perform safety functions during normal plant operation and for design basis events, and their major safety functions.

3. DEFINITION OF SAFETY RELATED SYSTEMS

3.1 Definition of Safety Related Systems

The safety objective for the design of a nuclear power plant, including the ACR, 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. The systems and structures that perform functions to maintain releases within regulatory limits are called safety related systems.

A National Standard of Canada, CAN/CSA N286.0 "Overall Quality Assurance Program Requirements for Nuclear Power Plants"(Reference [1]) states: *"the term "safety related system" covers a broad range of systems, from those having very important safety functions, to those with a less direct effect on safety. The larger the potential radiological safety effect, due to system failure, the stronger the "safety related" connotation."* This standard 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."*

3.2 Identification of Safety Related Systems

To satisfy the nuclear safety objective, the following fundamental nuclear safety functions (Control, Cool, Contain and Monitor) must be performed during normal 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).

The systems that perform the above safety functions are identified as safety related systems and structures.

4. CLASSIFICATION OF SAFETY RELATED SYSTEMS

4.1 International Safety Classification Principles

The ACR takes the International Atomic Energy Agency (IAEA) nuclear safety standards into account during the design. The IAEA document NS-R-1 "Safety of Nuclear Power Plants" outlines the principles for classification of safety related systems as follows:

"5.1 All structures, systems and components, including software for instrumentation and control (I&C), that are items important to safety shall be first identified and then classified on the basis of their function and significance with regard to safety. They shall be designed, constructed, and maintained such that their quality and reliability is commensurate with this classification.

5.2 The method for classifying the safety significance of a structure, system, or component shall primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment, with account taken of factors such as:

(1) the safety function(s) to be performed by the item;

(2) the consequences of failure to perform its function;

(3) the probability that the item will be called upon to perform a safety function;

(4) the time following a PIE (postulated initiating event) at which, or the period throughout which, it will be called upon to operate."

4.2 Application of Safety Classification in Design

The safety classification approach for CANDU plants is mainly directed at identifying the systems or structures that perform a safety function, and then grouping these systems into broad categories of systems that perform functions of similar importance. These broad categories are based on the following types of systems:

1. Systems or structures that must perform a safety function in the short term (i.e. immediately) to avoid a release that would significantly exceed the regulatory dose limits (e.g. shutdown in response to a failure causing an increase in power, injection of water to cool the fuel in response to a major pressure boundary failure). Generally, automatic actions are necessary to perform the safety function, although manual actions may also be needed in the longer term or for less severe design basis events. These systems are called "Safety Systems" (included in Category 2a and 2b in Section 4.3).
2. Systems or structures that perform a supporting role for the above systems, in the longer term (i.e. not essential immediately after a design basis event). Although automatic actions may be involved in providing its safety function, loss of the safety function will not impair the function of the Safety Systems defined above. These systems are called "Safety Support Systems" (included in Category 2c in Section 4.3).
3. Systems or structures that perform safety functions during normal operation of the plant, or following design basis events, other than the Safety Systems and Safety Support Systems defined above. Loss or failure of these systems may require mitigation by the Safety Systems and Safety Support Systems (included in Category 1 and 2 in Section 4.3).

Design requirements are applied to the above broad categories through regulatory documents or standards. The requirements applied to the systems or structures are based on the importance of the safety function being performed, the characteristics of the system, and the required reliability of the system, and are not based directly on their safety classification. For example, systems are qualified only if required to perform their function during unusual conditions caused by the design basis event for which they are credited (e.g. earthquake, harsh environment), and pressure boundary standards are applied based on the consequence of failure of that pressure boundary (e.g. ASME Section III is applied to heat transport system pressure boundary, ASME/ANSI B31.1 is applied to cooling water system pressure boundaries). A quality assurance program is applied to all safety related systems and structures to ensure that the design requirements are satisfied and the expected reliability is achieved.

During the design of safety related systems and structures, both safety related and non-safety requirements are applied in an integrated fashion through the preparation of a detailed design requirements document for each safety related system and structure.

4.3 Definition of Safety Categories

To satisfy the safety classification principles outlined above, safety related systems and structures are identified in terms of two categories, Preventative or Protective, defined 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. (Note that this category includes the Safety Systems for fuel cooling and containment, but also includes other safety related systems used for accident mitigation.)

   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

     These consist of four systems provided specifically to mitigate the consequences of an accident, which must perform their safety functions immediately after an event. They are the most important of the safety related systems. They are Shutdown System One, Shutdown System Two, Emergency Core Cooling, and Containment.

   - Safety Support Systems

     These systems provide services needed for proper operation of the Safety Systems (e.g., electrical power, cooling water), and may also perform safety and non-safety functions during normal operation of the plant.

5. IDENTIFICATION AND CLASSIFICATION OF SAFETY RELATED SYSTEMS AND STRUCTURES

A conceptual description of the systems used to perform the safety functions is presented below.

The detailed safety classification and major safety functions of the safety related systems and structures are shown in Table 1. During the application of these general requirements to the plant, more detailed or additional safety functions are identified, including those arising from safety analyses and probabilistic safety assessments, which are shown in a design requirements document for each individual system. Safety requirements are applied to each system based on regulatory requirements, codes and standards, safety analyses (deterministic and probabilistic), and customer requirements, taking into account the importance of the safety functions.

It is noted that many systems and structures in Table 1 also have a radiation protection function for operators, in terms of shielding, which is not reflected in the table, due to the numbers of systems involved and the complexity of this function. This aspect does not affect the classification of the systems and structures.

5.1 Conceptual Description of Safety Related Systems and Structures

5.1.1 Reactor Shutdown

For normal plant operation or anticipated operational occurrences, the Reactor Regulation System (RRS), which is part of Plant Control, shuts the reactor down or reduces reactor power either manually or automatically.

For design basis events, the reactor is shut down by either of 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 is designed so 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 occur.

5.1.2 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 (LTC). Refer to Figure 1 for a schematic representation of the pathways for the transfer of heat from the fuel in the heat transport system to an ultimate heat sink.

For accident conditions or external events, heat is removed from the fuel by the steam system, and/or by the two sub-systems of the emergency core cooling system (ECC), the emergency coolant injection system (ECI) and the long term cooling system.

If the ECC system fails, the moderator system removes heat from the fuel after the pressure tubes contact the calandria tubes due to sagging, as part of severe accident management. In the long

term, the shield cooling system can also be used to remove the decay heat that is conducted through the calandria shell.

The steam system removes heat to cool the reactor during normal and accident conditions. The major components that perform the heat removal function are the steam generators, the feedwater supplies, and the main steam safety valves (MSSVs).

For normal plant conditions, feedwater is supplied from the auxiliary feedwater pumps following a reactor shutdown. The main feedwater pumps are not safety related, although they will remain available if appropriate conditions and services (e.g. if Class IV power remains available) to them are maintained. The auxiliary feed pumps are sufficient to remove stored and decay heat, in conjunction with the stored inventory in the steam generators at the time of reactor shutdown.

For accident conditions, the auxiliary feedwater pumps in the main feedwater system are backed up by the reserve water system. If the main feedwater system fails, the reserve water system provides an independent supply of feedwater by gravity to the steam generators, with an inventory suitable until an alternative heat sink can be established.

The MSSVs are used to reject the heat to an 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 for maximum heat removal rate in response to a design basis event. This depressurization allows feedwater to be supplied at low pressure after initial heat removal, and also rapidly cools and depressurises the heat transport system to assist the ECI or moderator systems in cooling the fuel.

The ECC System detects a Loss of Coolant Accident (LOCA), refills the fuel channels if voiding has occurred, 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 using the long term cooling system (LTC). The ECC system also opens the MSSVs to assist in the rapid depressurization of the heat transport system, to facilitate injection to the heat transport system. The LTC pumps and heat exchangers are cooled by the recirculated cooling water system (RCW). LTC can be cooled from either of the two divisions of the RCW system.

The LTC system is also used for long term cooling of the heat transport system after a normal reactor shutdown and accidents with the HTS pressure boundary intact.

During normal operation the Shield Cooling System removes the nuclear heat from the end shield and shield tank. The system also removes heat transferred by conduction from the heat transport system and from the moderator system. The system provides sufficient cooling to prevent high stresses/deformation under normal and abnormal conditions to maintain the integrity of the reactor structures.

The moderator system maintains fuel channel integrity by providing circulation through the calandria and heat removal through its heat exchangers to the RCW following a combination of events involving a loss of coolant accident and loss of ECC. This heat sink is a part of severe accident management. If the moderator system fails, the shield cooling system will provide heat removal capability as a passive heat sink for severe accident management.

The reserve water system provides water to the ECC sumps to ensure adequate net positive suction head for the long term cooling pumps, to the steam generators to back up the feedwater system, and to the moderator system, shield cooling system, and heat transport system to replenish inventory loss.

5.1.3 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 elements, 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 the 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 Reactor Building. A continuous containment envelope is established using a combination of structures, isolation devices, and metallic extensions of the containment envelope.

For containment cooling, qualified local air coolers (LACs) will gradually reduce the high pressure/temperature/humidity inside the Reactor Building after a LOCA or MSLB and continue long term cooling. Cooling water for the LACs is provided from the RCW.

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

5.1.4 Monitoring and Control Systems

All events, including the seismic event, will be handled from the main control room (MCR). Events causing MCR uninhabitability (e.g. fires, hostile takeover, etc.) will be handled from the Secondary Control Building (SCB) 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, and the safety classification will reflect its use for this purpose.

5.1.5 Safety Support Systems

The major support services for the safety related systems include the cooling water systems, the electrical system, the compressed air systems, and the ventilation systems.

Cooling Water Systems

The cooling water systems consist of two independent divisions of raw service water (RSW) and recirculated cooling water (RCW), each of which can be interconnected to provide a backup for each other where redundant cooling water supplies are needed for reliability reasons. The RSW system is a once-through system that draws water from the ultimate heat sink[1] to cool the RCW heat exchangers. The RCW, 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 system is a closed loop system which provides cooling water to equipment across the plant, including both safety related loads and other 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 system via heat exchangers.

Electrical System

The electrical system also consists of two divisions which provide electrical energy to power production related equipment and safety related systems, each of which can be interconnected to provide a backup for each other where redundant supplies are needed for reliability reasons.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 seismically qualified AC power, supplied from Class IV and backed up by dedicated standby diesel generators (two for each division),
- Class II is a stored energy, seismically qualified, highly reliable AC power supply and
- Class I power is a stored energy, seismically qualified, highly reliable DC power source.

The Class I, II, and III electrical power supplies are 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.

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, where necessary for reliability, to supply instrument air to essential users during a loss of the normal air supply.

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.

---

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

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 is isolated to establish the containment envelope.

5.2 Requirements for Safety Related Systems

Each safety related system or structure is designed to satisfy a set of requirements derived from regulatory requirements, recognized codes and standards, and safety analyses. Conceptual requirements are defined that ensure that the safety function assigned to that system is addressed. Detailed performance requirements are then established for each safety related system, to ensure that all safety related requirements are satisfied. A quality assurance program is applied to the design process for all safety related systems [Reference 1].

Safety related systems or structures that perform safety functions during normal plant operation, are 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.

Safety related systems that perform safety functions to mitigate an event are designed to be highly reliable, with reliability targets established using probabilistic safety assessments.

Table 1 includes some of the conceptual safety requirements used to define the safety functions and performance requirements for safety related systems. Other requirements may be applied, based on customer requirements and the regulations relevant to the location of the plant.

6. REFERENCES

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

[2] Safety Design Guide 108-03650-SDG-001 “Safety Related Systems”

Table 1
List of Safety Related Systems

ASI	Safety Category	System or Structure	Safety Function
20000	BUILDINGS AND STRUCTURES		
21000	1(d), 2(b)	Reactor Building (Also see 68400)	Provides a barrier to the release of radioactive materials following a release within the containment envelope. The reactor building is designed with a leak rate that will satisfy public dose criteria for events involving releases of radioactive materials inside the building. Retains its structural integrity for all internal and external design basis events, including a main steam line break, to enable safety related components to continue to function as required. Protects safety related systems from environmental conditions and severe events occurring outside the reactor building. Supports safety related systems inside the reactor building (internal structures).
21600	1(d), 2(b)	Special Equipment (Airlocks, Shielding Doors, Blowout Panels, Atmosphere Barriers, Equipment Hatch)	Provides a barrier to the release of radioactive materials, and a pressure boundary for high pressures in the reactor building. Protects plant staff from radiation exposure by providing a means of exit from the reactor building after an event.
22000	1(d)	Turbine Building	Protects safety related systems from the consequences of events occurring in the turbine building.
23005	1(d)	CCW/RSW Pumphouse	Protects safety related systems against the effects of external events and provides acceptable environmental conditions for systems and components housed within.
24000	1(d)	Reactor Auxiliary Building	Protects safety related systems against the effects of external events and provides acceptable environmental conditions for systems and components housed within.

ASI	Safety Category	System or Structure	Safety Function
24250	1(b)	Spent Fuel Bay	Maintains the fuel bay inventory for fuel cooling, protects the fuel from external events, and limits radioactive release from the bay.
24xxx	1(d)	MSSV/MSIV Structure	Protects safety related components (MSSVs and MSIVs) from the effects of environmental conditions.
25000	1(d)	Control Building	Protects safety related systems against the effects of external events and provides acceptable environmental conditions for systems and components housed within.
25000	1(d)	Secondary Control Building (see 66600)	Protects safety related systems that perform monitoring and control functions for events involving loss of function of the main control room.
28003	1(d)	Standby Generator Area Structure	Protects safety related systems against the effects of external events and provides acceptable environmental conditions for systems and components housed within.
30000	REACTOR, REACTOR SYSTEMS AND AUXILIARIES		
31000	1(a), 1(d)	Reactor (see 32100 and 33100)	Maintains the integrity of the heat transport system and provides support for reactor control mechanisms.
32000	Moderator Systems and Auxiliaries		
32100	2(c), 1(d)	Moderator Systems	During normal operation, removes heat from the reactor structures to maintain structural integrity. Maintains fuel cooling during accident conditions, including a LOCA combined with a loss of the ECC system, as part of severe accident management.
32200	1(d)	(Moderator) Purification System (includes Deuteration and Dedeuteration)	Maintains the shutdown condition of the reactor after an SDS2 trip, by stopping the moderator purification process, during accident conditions or other events.
32300	1(d)	(Moderator) Cover Gas System	Prevents the accumulation of explosive levels of deuterium in the calandria during normal plant operation. Maintains subcooling conditions in the moderator, by maintaining suitable cover gas pressure, to permit fuel cooling after a loss of coolant accident, as part of severe accident management.

ASI	Safety Category	System or Structure	Safety Function
32700	2(c)	(Moderator) Liquid Poison Systems	Maintains the reactor in a shutdown condition in the long term by addition of negative reactivity through operator action.
33000	Heat Transport Systems and Auxiliaries		
33100	1(a), 1(c), 2(b)	Heat Transport Circuit	Maintains the integrity of the pressure boundary, to permit heat removal from the fuel during normal operation and accident conditions, including via thermosyphoning. During normal operation, provides a barrier to the release of radioactive materials to ensure that doses to plant staff remain within acceptable limits.
33310	1(c), 1(d)	Heat Transport Pressure and Inventory Control System	Maintains adequate inventory in the heat transport system to ensure fuel cooling during normal plant operation and anticipated operational occurrences. Maintains the integrity of the heat transport system pressure boundary. 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.
33340	1(d)	HTS Pump Seal Circuit	Maintain the integrity of the heat transport system pressure boundary. Provides cooling to the heat transport pump seals.
33350	1(d)	Heat Transport Purification System	Removes the radioactive substances from the reactor coolant, including activated corrosion products and fission products leaking from the fuel.
33540	1(d)	Hydrogen Addition Circuit	Provides suitable chemical conditions in the heat transport system to maintain pressure boundary integrity.

ASI	Safety Category	System or Structure	Safety Function
34000	Auxiliary Systems		
34110	1(c), 1(d)	Shield Cooling System	During normal operation, removes heat from the end shield and shield tank to maintain structural integrity. Provide a passive heat sink capability during a severe accident event.
34300	Emergency Core Cooling System		
34320	Safety System 2(b)	Emergency Coolant Injection System	Provides inventory make-up to the heat transport system in the short term (high-pressure injection stage) of a LOCA to maintain fuel cooling. Opens the MSSVs to assist in the rapid depressurization of the HTS to facilitate injection. The system is capable of replenishing heat transport system coolant inventory for events that do not involve a LOCA (e.g. for post-DBE make-up to the heat transport system for pre-existing leaks).
34340	2(b), 2(c)	Reserve Water System	Stores water for make-up to the HTS, the LTC system (including via ECC sumps), moderator and shield cooling systems, and as a backup feedwater supply for the steam generators.
34350	1(a), 1(c) Safety System 2(b)	Long-Term Cooling System	Removes decay heat from the HTS in the long term for normal plant shutdown, transients, and accidents with the HTS pressure boundary intact. Provides fuel cooling in the long term (recovery stage) of a LOCA.
34410	1(c), 1(d)	(Spent Fuel Bay) Cooling and Purification System	Maintains cooling of irradiated fuel during normal plant operation and accident conditions. Provides makeup water to the spent fuel bay if the inventory is depleted via vaporization after a seismic event (alternatively, another qualified water makeup source may perform this function).
34710	2(a)	Liquid Injection Shutdown System	This system is part of 68300
34980	1(c)	Annulus Gas System	Maintains suitable conditions in the annulus during normal plant conditions to ensure that deterioration of the pressure tubes does not occur. Monitors the integrity of the HTS pressure tubes by leak detection.

ASI	Safety Category	System or Structure	Safety Function
35000	Fuel Handling and Storage		
35100	1(d)	New Fuel Transfer and Storage	Limits the release of radioactive material by maintaining the containment boundary. Prevents fuel criticality during storage and transfer of the fuel.
35200	1(a), 1(d)	Fuel Changing	Maintains the integrity of the heat transport system pressure boundary. Provides fuel cooling during transfer to the fuel storage bay. Limits the release of radioactive material by maintaining the containment boundary.
35300	1(c), 1(d)	Spent Fuel Transfer and Storage	Prevents draining of the inventory in the irradiated fuel storage bay. Provides fuel cooling during transfer to the fuel storage bay. Limits the release of radioactive material by maintaining the containment boundary following a postulated accident.
35360	1(c), 1(d)	Storage Bay (spent fuel tray and supports)	Protects fuel from criticality and damage and enable cooling of irradiated fuel during normal plant operation and accident conditions.
35730	1(d)	FM Cable and Hose Management System	See 35200
36000	Steam Generator Systems		
36100	1(c), 2(c)	Steam and Relief Systems	Removes heat from the heat transport system to provide fuel cooling. Provides overpressure protection for the steam generators.
36310	1(d)	Steam Generator Blowdown System	Maintains the capability to remove heat from the heat transport system
37000	1(a)	FUEL	Maintains integrity of the fuel cladding in the core and bundle integrity.
40000	TURBINE – GENERATOR AND AUXILIARIES		
41600	1(d)	Oil Fire Protection System	Provides fire protection to prevent fire s from spreading to safety related systems

ASI	Safety Category	System or Structure	Safety Function
43000	Feedwater and Auxiliary Steam Systems		
43230	1(c), 2(c)	Feedwater System (includes Auxiliary Feedwater, Deaerator and Deaerator Storage Tank)	Provides auxiliary feedwater to the steam generators to remove residual and decay heat after reactor shutdown, in conjunction with the inventory contained in the steam generator.
50000	ELECTRIC POWER SYSTEMS		
50000	1(c), 2(c)	Electric Power System	Provides electrical power to enable safety related systems to perform their safety functions during normal operation and following an event, as required.
52000	2(c)	Standby Generators	Maintains the electrical power generating capacity as needed by the safety related systems following loss of the normal electrical power supply.
53000	1(c), 2(c)	Distribution System	Provides electrical power to enable systems to perform their safety functions as required.
56000	1(d)	Lighting and Building Service Systems	Maintains lighting and other services to enable operating staff to perform monitoring and control functions for safety related systems.
57000	1(c), 2(c)	Cabling System	Maintains power supply to enable safety related systems to perform their safety functions as required.
57600	2(b)	(Electrical) Containment Penetrations	Maintains a containment barrier to the release of radioactive material.
60000	INSTRUMENTATION AND CONTROL		
61500		Seismic Instrumentation Equipment	Monitors seismic activity.
63101	1(c)	Channel Flow Measurement	Monitors the coolant flow and temperature to confirm adequate fuel cooling during normal plant operation.
63102		Channel Temperature Monitoring	

ASI	Safety Category	System or Structure	Safety Function
63103	1(c)	Gaseous Fission Product Monitoring	Continuously monitors the integrity of the fuel in the reactor by detecting defective fuel.
63105	1(c)	Delayed Neutron Monitoring System	Locates small fuel defects while reactor is at power.
63700	1(c), 1(d)	Plant Control (includes Reactor Regulating System)	Provides control and monitoring of safety related systems during normal plant operation. Controls the reactor within specified conditions during normal operation to prevent loss of regulation incidents. Shuts down the reactor for events anticipated to occur frequently during plant life. During accident conditions, fails safe in a manner that does not put the plant in a state exceeding the shutdown capability.
66000	1(c), 2(c)	Control Centre	Provides control and monitoring during normal operation and after all accident conditions for which the control room remains available and habitable.
66600	2(c)	Secondary Control Building (SCB)	Provides the capability to shutdown the reactor and maintain it in a safe shutdown state, and monitor the plant under accident conditions.
67147	1(d)	Fire Detection and Alarm System	Provides the capability to detect fires that could potentially damage safety related systems.
67314	2(b)	Containment Isolation	Establishes the containment barrier for open pathways from the heat transport system or containment atmosphere to the environment, which may be normally open, or become open during a design basis accident.
68200	2(a) Safety System	Shutdown System No. 1 (SDS1)	Shuts the reactor down and maintains it in a safe shutdown condition.

ASI	Safety Category	System or Structure	Safety Function
68300	2(a) Safety System	Shutdown System No. 2 (SDS2)	
68400	2(b) Safety System	Containment System (see 67314 for Containment Isolation System)	Provides a barrier to the release of radioactive materials within the containment envelope. (Also see 21000, 67314, 73140).
68480	1(d), 2(c)	Hydrogen Control System	Maintains the integrity of the containment envelope and safety related systems by controlling the concentration of hydrogen and or oxygen following an accident.
68570	2(b)	Second Crash Cooldown System	Depressurizes the secondary side of the steam generators by opening the MSSVs to assist the fuel cooling function.
68631	2(b)	Containment Ventilation Isolation System	Establishes the containment barrier for normally open ventilation ducts.
68900	2(c)	Post Accident Management	Monitors the condition of the plant after an accident and provides information to the operator.
70000	COMMON PROCESSES AND SERVICES		
71300	1(c), 1(d), 2(c)	Service Water Systems (Raw Service Water system and Recirculated Cooling Water system)	Provides cooling water to safety related systems to prevent the occurrence of accident conditions, and to mitigate the effects of accident conditions.
71400	1(d)	Fire Water Protection System (Fire Water Supply System)	Detects fires and prevents them from spreading to safety related systems. Provides a fire water supply.

ASI	Safety Category	System or Structure	Safety Function
71900	1(d)	Chilled Water System	Provides acceptable environmental conditions for safety related systems.
72200		Fuel Oil Systems	Provides fuel for standby and emergency generators
73110	1(d), 2(c)	(Reactor Building) Cooling System	Provides cooling to the R/B during plant normal operation. Provides cooling of the RB during and following design basis events, as required. Circulates the air to prevent build-up of flammable or explosive hydrogen concentrations. Provides acceptable environmental conditions for safety related systems.
73120	1(c), 1(d)	(Reactor Building) Ventilation System	Provides acceptable environmental conditions for safety related systems
73140	2(b)	Reactor Building Containment Isolation	See 68400
73150	1(d)	(Reactor Building) Heating System	Provides acceptable environmental conditions for safety related systems
73360	1(d)	RSW Pumphouse Heating System	Provides acceptable environmental conditions for safety related systems.
73370		RSW Pumphouse Ventilation System	
73410	1(d), 2(c)	Heating System	Provides acceptable environmental conditions for safety related systems.
73420		Ventilation System	
73450	1(d), 2(c)	Main Control Area (MCA) (Heating and Cooling)	Provides cooling to safety related control and display components.
73460	2(c)	Secondary Control Building (SCB) (Heating and Cooling)	Provides cooling to safety related control and/or display components.
73900	1(d), 2(c)	Miscellaneous Structures (Heating and Cooling)	Provides cooling to protect safety related systems.

ASI	Safety Category	System or Structure	Safety Function
75120	1(d), 2(c)	Instrument Air	Provides instrument air to safety related systems to prevent the occurrence of accident conditions and to mitigate the effects of accident conditions.
75600	1(d)	Combustible Gases	Located to prevent damage to safety related systems during a failure which causes a fire.
76000	1(d)	Material Handling (Cranes and Hoists)	Located to prevent damage to safety related systems during an earthquake event.
78200		Fuel Oil Systems	See specific user system
79000	1(d)	RADIOACTIVE WASTE MANAGEMENT	Ensures that regulatory dose limits are not exceeded for normal plant operation and design basis events, including earthquakes.

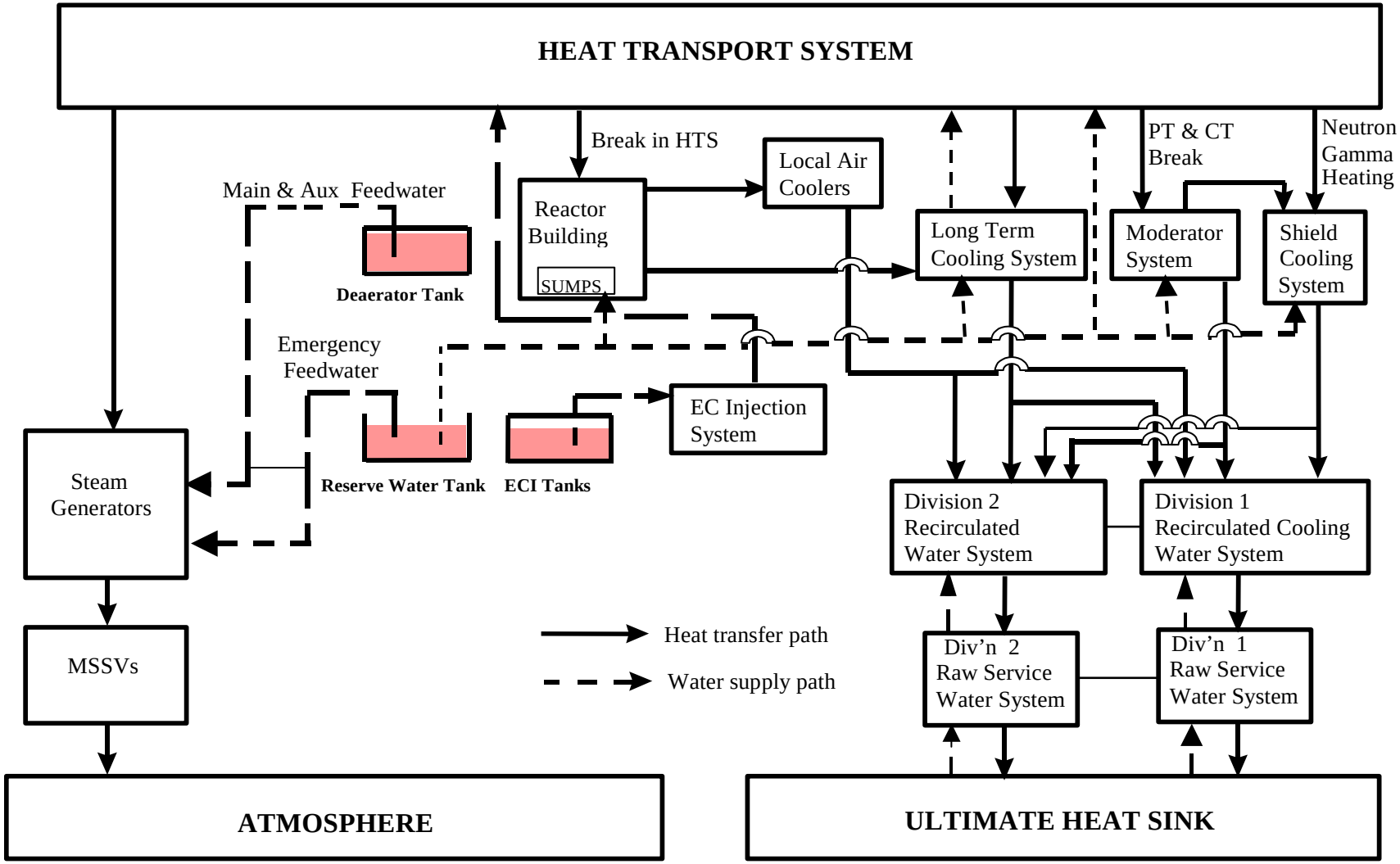

Figure 1 Schematic of Safety Related Systems which Transfer Residual Heat to an Ultimate Heat Sink