Advanced CANDU Reactor Safety Design Approach

By Massimo Bonechi
Manager, Safety Engineering, ACR Development
Presented to US Nuclear Regulatory Commission
Washington DC
March 27, 2003

AECL TECHNOLOGIES INC.

Presentation Outline

- Defense-in-depth
- Safety design principles
- Safety design criteria
- Safety design implementation

Defense-In-Depth

- High-quality process systems to accommodate plant transients and to minimize the likelihood of accidents
- Reliable safety systems for reactor shutdown, emergency core cooling and containment
- Reliable safety support systems to provide services to the safety systems and other mitigating systems
- Backup systems for heat sinks and essential controls
- Passive heat sinks to increase resistance against severe accidents

Safety Design Principles

- Separation and diversity of reactor shutdown systems and heat sinks
- Reliability of safety systems
- Redundancy and independence of divisions within safety systems and safety support systems
  - a division is a subset of a system, which alone is sufficient to carry out the safety function of the system
  - meets single failure criterion
- Seismic and environmental qualification of essential systems

Safety Design Criteria

Reactor Nuclear Design

- The reactor core shall be designed so that
  - Power reactivity coefficient is negative in the power operating range
  - Full-core void reactivity is small and negative to provide a good balance of nuclear protection between loss-of-coolant accidents and fast cooldown accidents
- The flux profile across the core shall be such as to minimize the required number of reactivity control devices and hence the demand on the reactor control system

Reactor Mechanical and Thermal Design

- The reactor components shall be designed with sufficient mechanical and thermal margins to assure that applicable acceptance criteria for fuel and fuel channel performance are not exceeded during transients and accidents
- All reactivity control devices shall be located in the low-pressure moderator so that their mechanisms do not penetrate the reactor coolant pressure boundary

Reactor Coolant System

- The highest quality nuclear codes and standards shall be applied to the design of the reactor coolant system so as to minimize the failure probability of the reactor coolant pressure boundary
- The reactor coolant system shall be provided with natural circulation capability to deal with transients and accidents involving loss of forced circulation

Reactor Shutdown

- Two independent shutdown systems shall be provided
- The two shutdown systems shall use diverse design and operating principles to the extent practical
- The shutdown systems shall be separated from the control systems. Sharing of sensing instrumentation between a shutdown system and a control system may be permitted if failure of the control system does not adversely affect the shutdown function
- The reliability of at least one shutdown system shall be no less than 0.999
- The shutdown systems shall be seismically qualified

Shutdown Heat Removal

- Systems shall be provided to remove shutdown heat following transients and accidents with the reactor coolant pressure boundary intact
  - A system for the short term, rejecting heat via the steam generators
  - Another system for the long term, rejecting heat to the cooling water systems
- The heat removal system required in the short term shall be automated
- Both heat removal systems shall be provided with two redundant and independent divisions (to meet single failure criterion)
- Both heat removal systems shall be seismically qualified

Emergency Core Cooling

- An emergency coolant injection system shall be provided to maintain adequate fuel cooling in the short term following loss of coolant accidents
- The emergency coolant injection system shall be automated with a reliability no less than 0.999
- The emergency coolant injection system shall meet the single failure criterion
- The emergency coolant injection system shall be seismically qualified

Emergency Core Cooling

- A long-term cooling system shall be provided to remove heat from the reactor for loss-of-coolant accidents, after exhaustion of the water sources for the emergency coolant injection system
- Switchover from the emergency coolant injection system to the long-term cooling system shall be automated
- The long-term cooling system shall be provided with redundant and independent divisions of water supplies and injection lines (to meet single failure criterion)
- The long-term cooling system shall be seismically qualified

Containment Boundary

- The containment boundary shall be designed to maintain the required leak-tightness for loss-of-coolant accidents
- The containment boundary shall be designed to maintain its structural integrity for main steam line breaks inside containment
- The containment boundary shall be seismically qualified

Containment Isolation

- A system shall be provided to close process lines that penetrate the containment boundary and are not required for accident mitigation actions, following a loss-of-coolant accident
- The containment isolation system shall be automated and provided with two redundant and diverse actuation signals
- The reliability of the containment isolation system shall be no less than 0.999
- The containment isolation system shall be seismically qualified

Containment Cooling

- A system shall be provided to remove heat from the containment atmosphere following events which release energy inside containment, to maintain the containment pressure below acceptable limits
- The containment cooling system shall be provided with two redundant and independent divisions (to meet single failure criterion)
- The containment cooling system shall be seismically qualified

Containment Hydrogen Control

- A system shall be provided to maintain the hydrogen concentration inside containment below acceptable limits following accidents
- The containment hydrogen control system shall be seismically qualified

Main Control Room and Secondary Control Building

- The main control room shall be provided with the capability for the operator to deal with all transients and accidents, including a design basis earthquake
- A secondary control building shall be provided to permit reactor shutdown, cooldown and essential monitoring functions for events that may render the main control room uninhabitable (fires, aircraft crash, hostile takeover)

Cooling Water

- Systems shall be provided to transfer heat from safety related loads in the unit to an ultimate heat sink under normal operating, transient and accident conditions
- The cooling water systems shall be provided with two redundant and independent water supplies (to meet single failure criterion)
- The cooling water supplies for safety support loads shall be seismically qualified

Electrical Power Systems

- Onsite electrical power systems shall be provided to supply power to safety related loads in the event of failure of the normal power supplies
- The onsite electrical power systems shall be provided with two redundant and independent divisions (to meet single failure criterion)
- The onsite electrical power supplies shall be automated and seismically qualified

Spent Fuel Storage

- Spent fuel storage shall assure that the fuel is covered with water at all times during normal operation, transients and accidents, so that decay heat is removed from the fuel and adequate radiation shielding is maintained
- Criticality in the spent fuel storage system shall be prevented by appropriate measures

Severe Accidents and Severe Core Damage Accidents

- *Severe accidents:* improbable accidents whose consequences are arrested at the channel boundary, therefore not compromising core coolable geometry
- *Severe core damage accidents:* even more improbable accidents where core damage progresses beyond preservation of the channel boundary

Severe Accidents and Severe Core Damage Accidents

- The moderator system shall provide a backup heat sink capable to maintain core coolability for *severe accidents* due to loss-of-coolant accidents combined with the unavailability of the emergency core cooling
- The moderator system and the shield water system shall have sufficient thermal capacity to slow down a *severe core damage* progression and allow time for the operator to implement severe accident management measures
- Passive makeup systems shall be provided for the moderator and the shield water to maximize the duration of their heat removal capability for *severe core damage accidents*

Safety Design Implementation

Inherent Safety Characteristics

- ACR maintains the traditional CANDU inherent safety characteristics
  - Natural circulation capability in the reactor coolant system to cope with transients due to loss of forced flow
  - On-power fueling reduces excess reactivity holdup
  - Reactivity control devices are in the low pressure moderator so their mechanisms do not penetrate the reactor coolant pressure boundary
  - Moderator backup heat sink maintains core coolability for loss-of-coolant accidents combined with the unavailability of the emergency core cooling (severe accident)

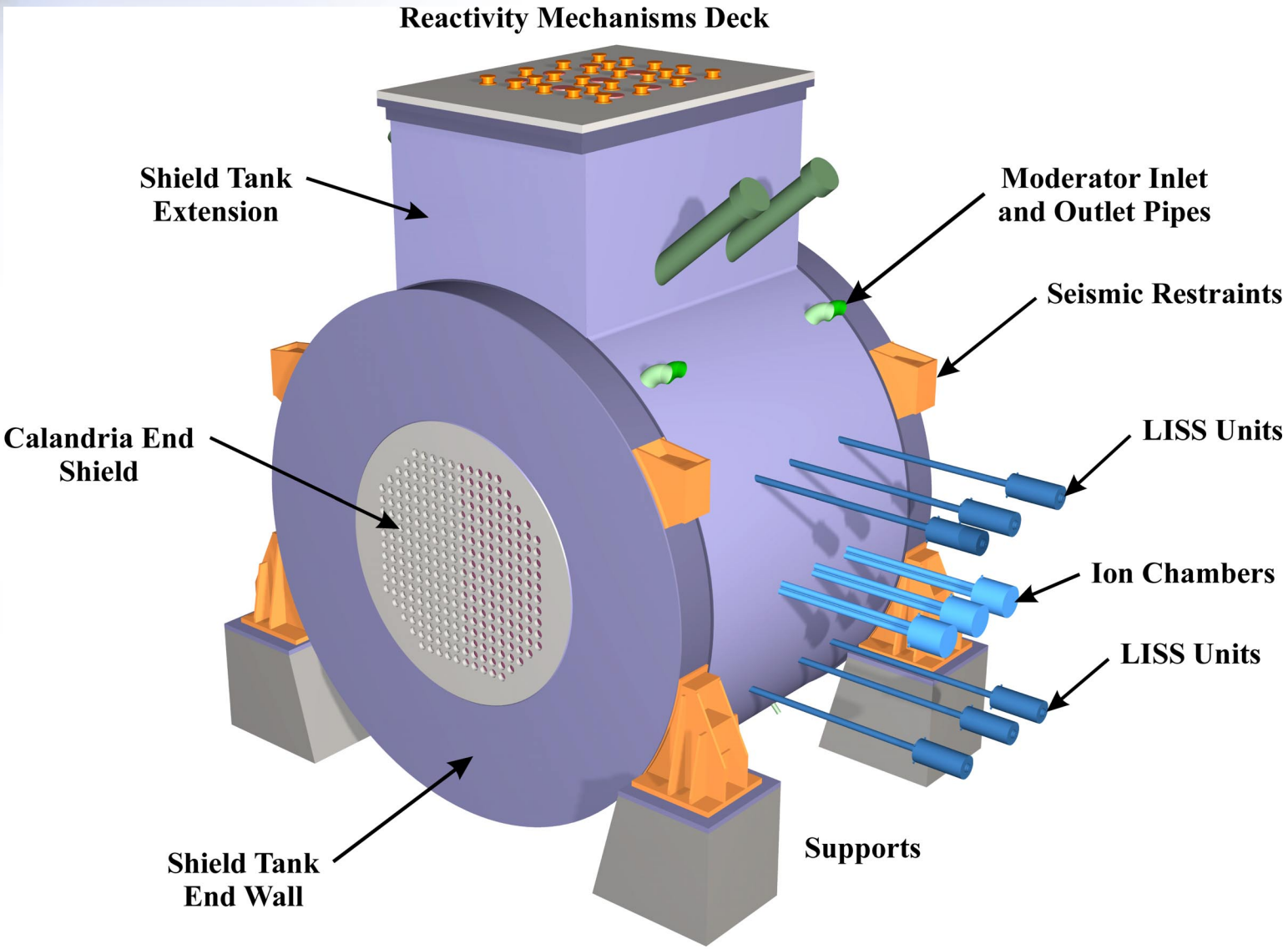
Inherent Safety Characteristics

- Additional inherent safety characteristics in ACR compared to existing CANDU plants:
  - Negative power reactivity coefficient
  - Small negative full-core void reactivity offers a good balance of nuclear protection between loss-of-coolant accidents and fast cooldown accidents
  - Very flat and stable flux across the core minimizes the demand on the reactor control system
  - Larger safety and operating margins due to the use of CANFLEX fuel with lower element rating and higher critical heat flux

Shutdown Systems

- Two independent and diverse shutdown systems
- Passive systems

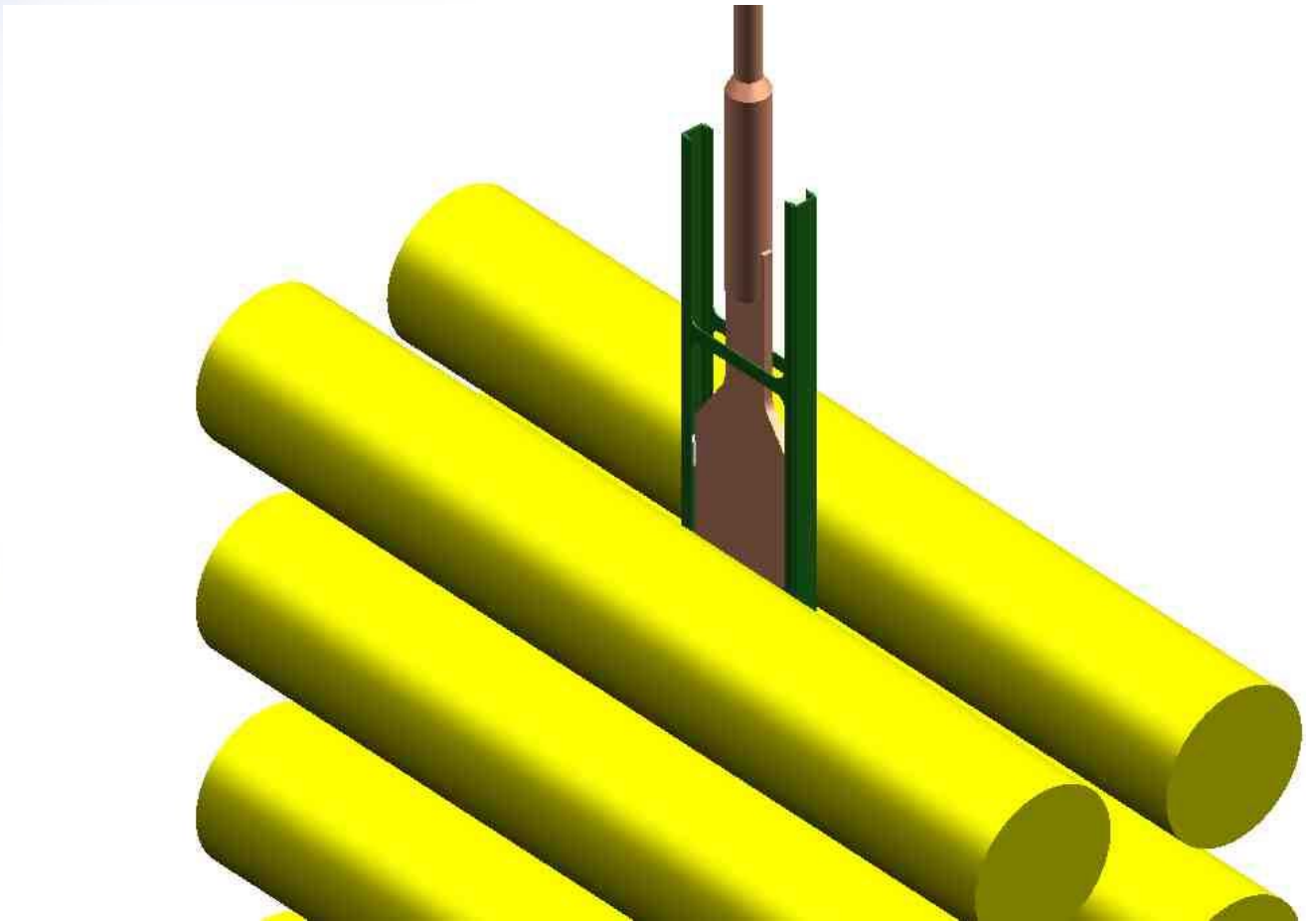
Reactor Assembly



Shutdown System 1

- Shutdown System 1 (SDS 1) consists of 20 mechanical shutoff rods that drop into the core by gravity upon reactor trip signal.
- SDS 1 inserts -50 mk to shut down the reactor after an accident

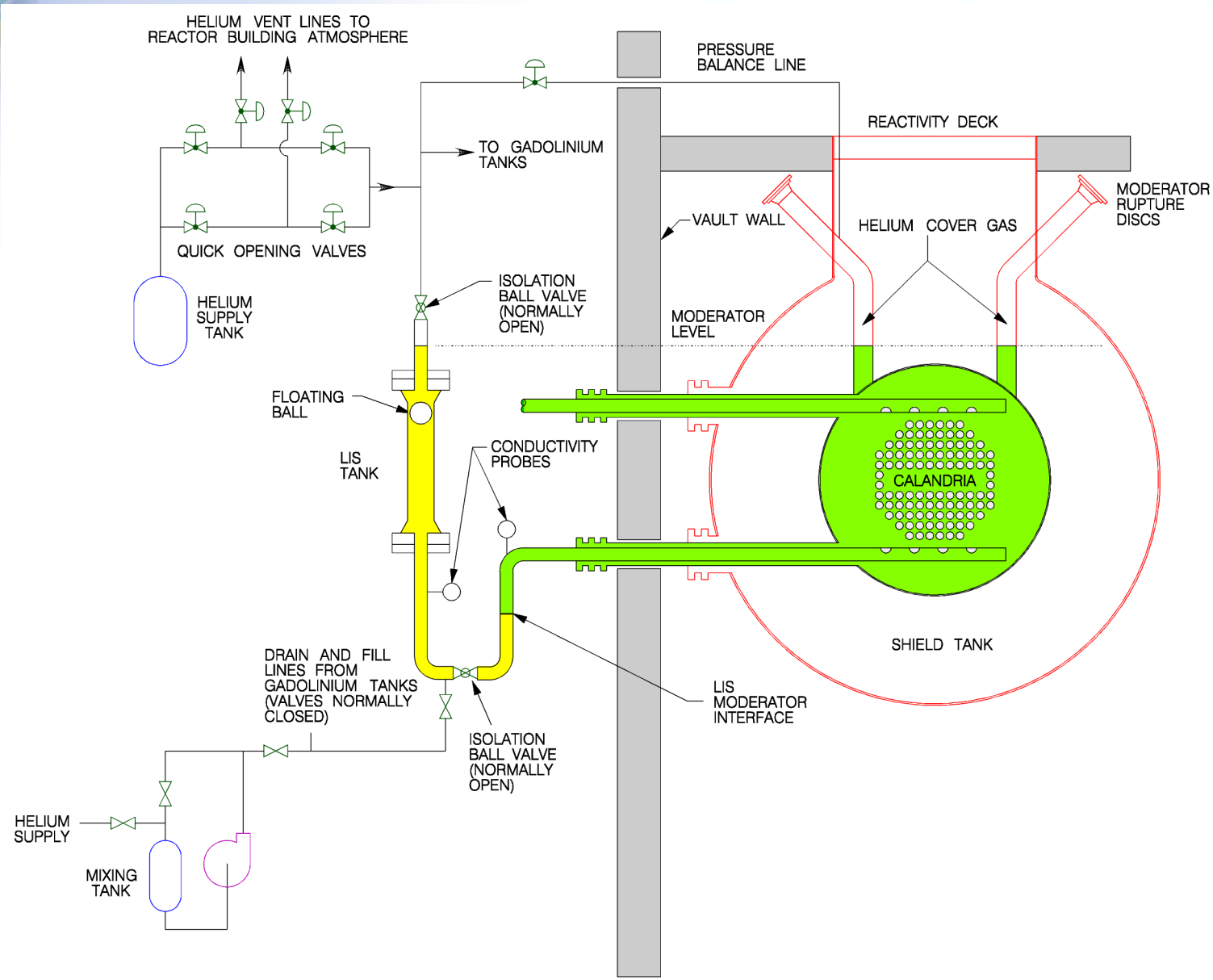
SDS 1 Shutoff Rod Unit



Shutdown System 2

- Shutdown System 2 (SDS 2) injects concentrated gadolinium nitrate solution into the low pressure moderator to render the core subcritical following postulated accidents.
- Injection is from pressurized tanks through nozzles traversing the calandria in the upper and lower reflector regions.
- SDS 2 is designed to inject -50 mk of reactivity to shut down the reactor after an accident, and contains enough gadolinium to inject -200 mk of reactivity to keep the reactor shut down.

Shutdown System 2



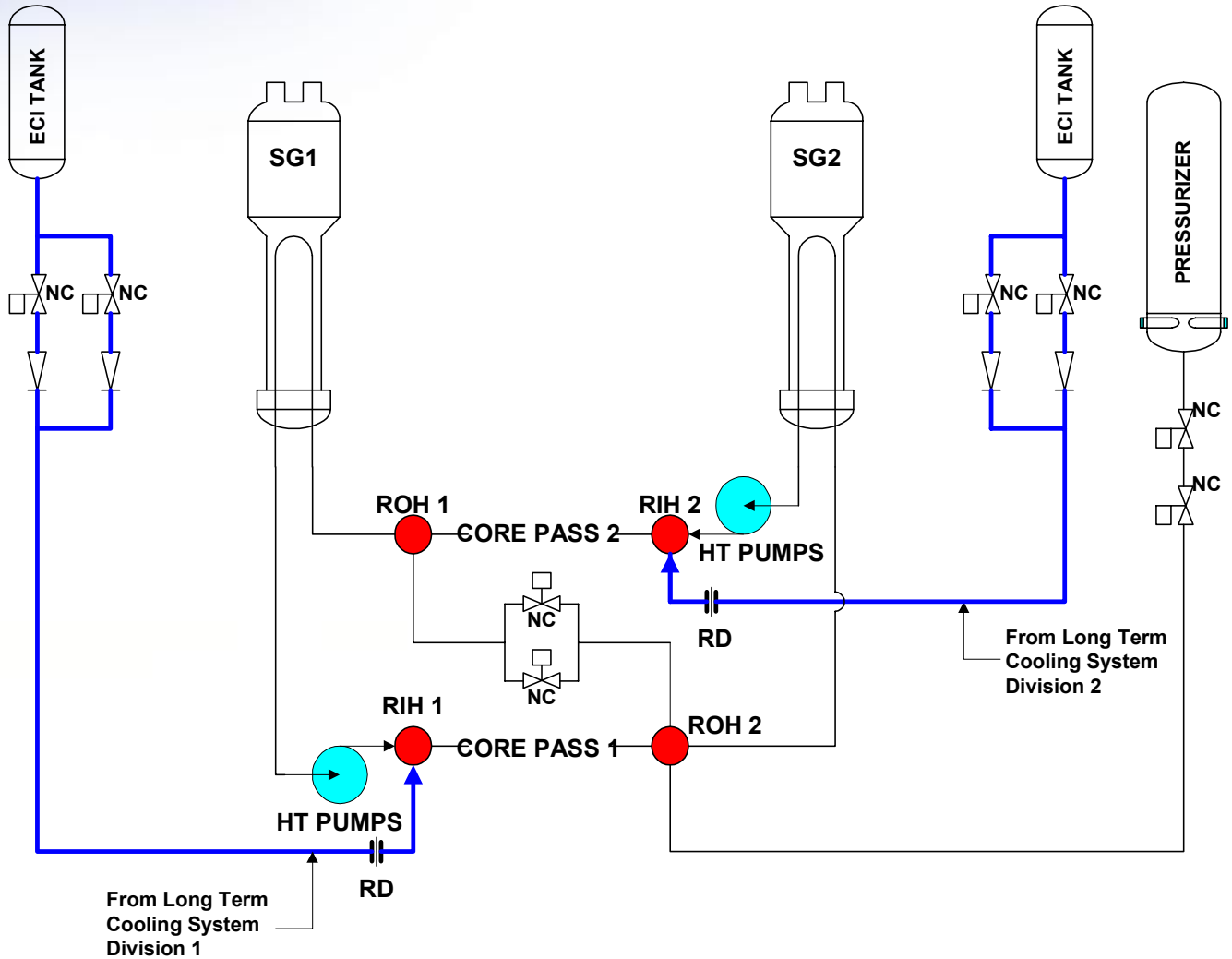
Emergency Core Cooling

- The Emergency Core Cooling (ECC) function is carried out by two systems:
  - Emergency Coolant Injection (ECI) System for high-pressure coolant injection after a Loss-of-Coolant Accident (LOCA)
  - Long Term Cooling (LTC) System for recirculation after LOCA

Emergency Coolant Injection System

- Passive injection from normally pressurized tanks.
- The ECI system has been simplified to further enhance reliability and performance:
  - use of passive one-way rupture discs at the interface with the reactor coolant system
  - injection into reactor inlet headers only
  - large interconnect line between reactor outlet headers to assist in establishing an effective cooling flow path

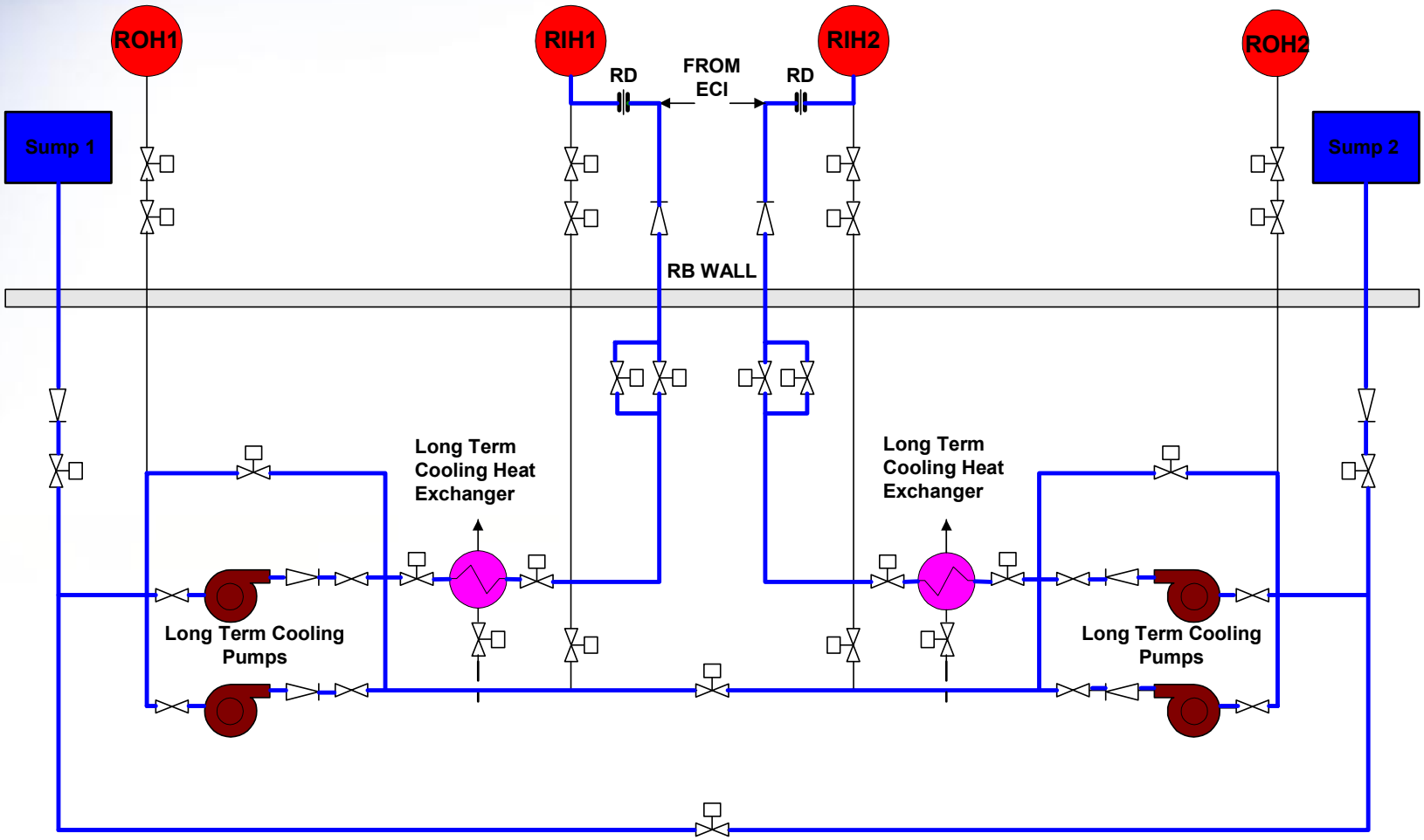
Emergency Coolant Injection System



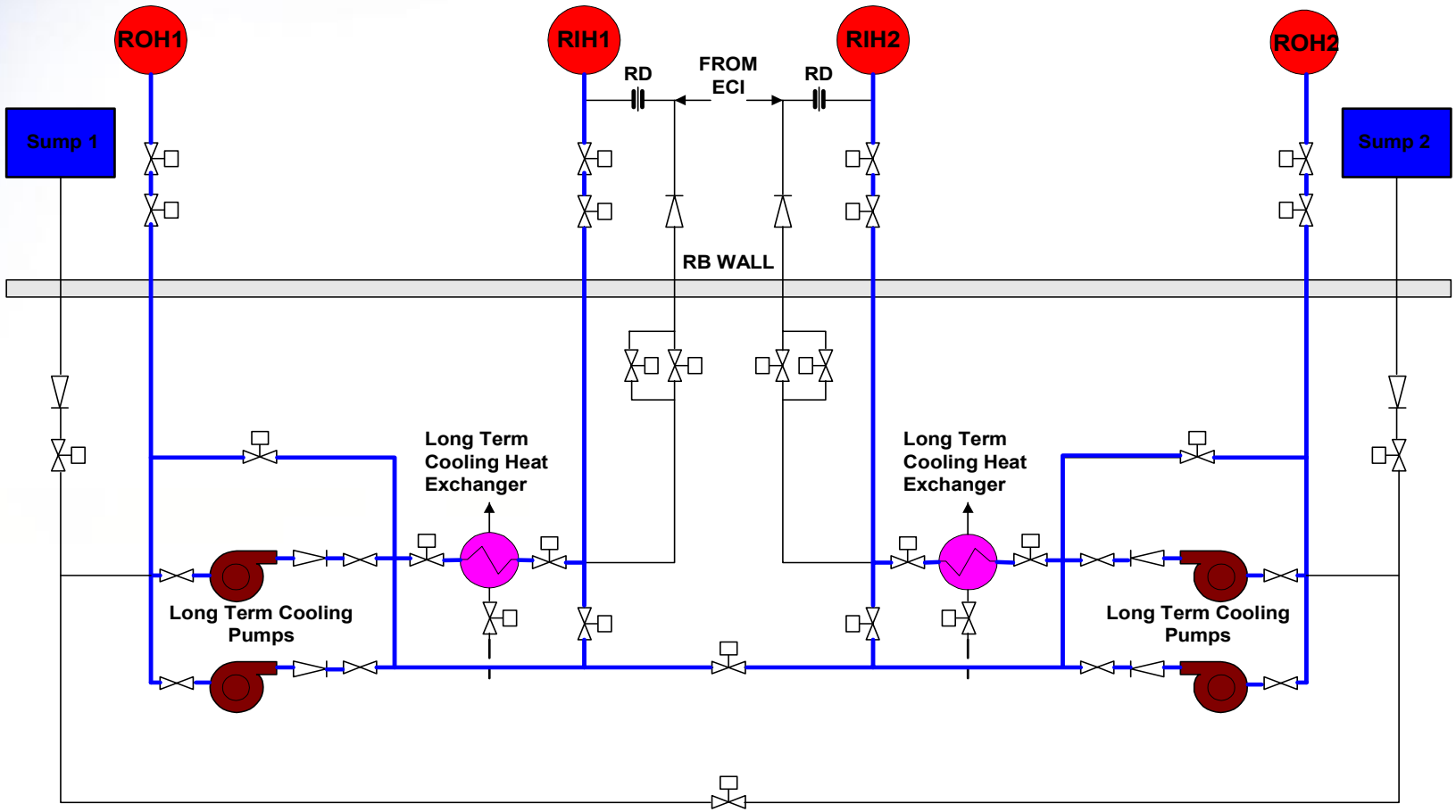
Long Term Cooling System

- Long Term Cooling (LTC) system provides fuel cooling in the long term (recovery stage) of a LOCA and removes long term decay heat for all conditions with the reactor coolant system (RCS) pressure boundary intact.
- Comprised of two redundant divisions located in separate areas of the reactor auxiliary building. LTC pumps are supplied power by the seismically qualified Class III electrical system.
- The LTC system serves also the function of shutdown cooling for cooldown after a normal shutdown.

LTC: Post-LOCA Recirculation



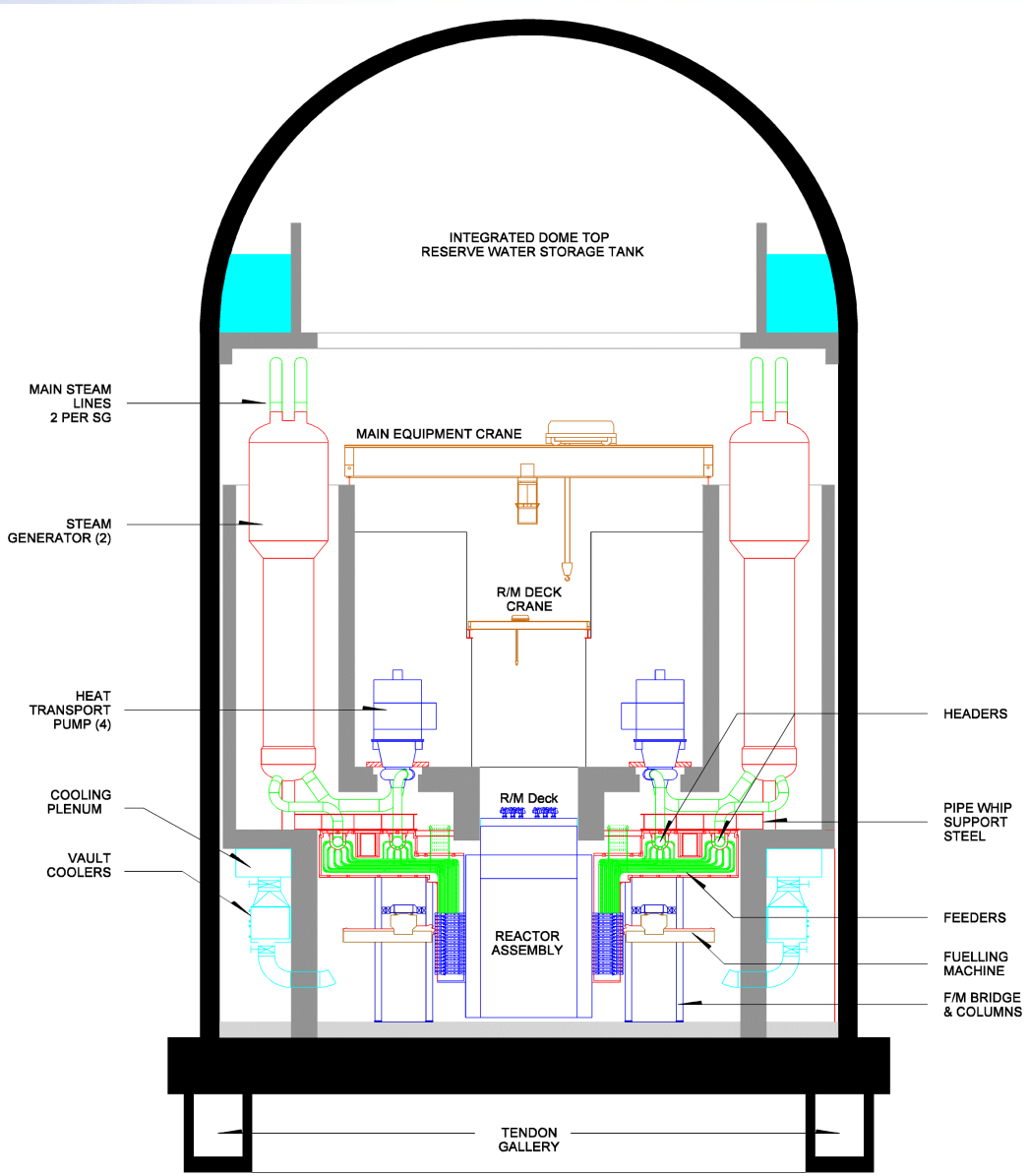
LTC: Cool-down



Containment

- Steel-lined, pre-stressed concrete reactor building structure designed for a low leakage rate of 0.2% volume/day while providing a pressure retaining boundary for LOCA.
- Containment isolation system automatically closes penetrations open to the reactor building atmosphere upon signals of high pressure or high radioactivity in the reactor building.
- Heat removal from the containment atmosphere after an accident is provided by the containment cooling system, comprised of local air coolers suitably distributed inside the reactor building.
- Hydrogen control is provided by passive auto-catalytic recombiners.

Containment



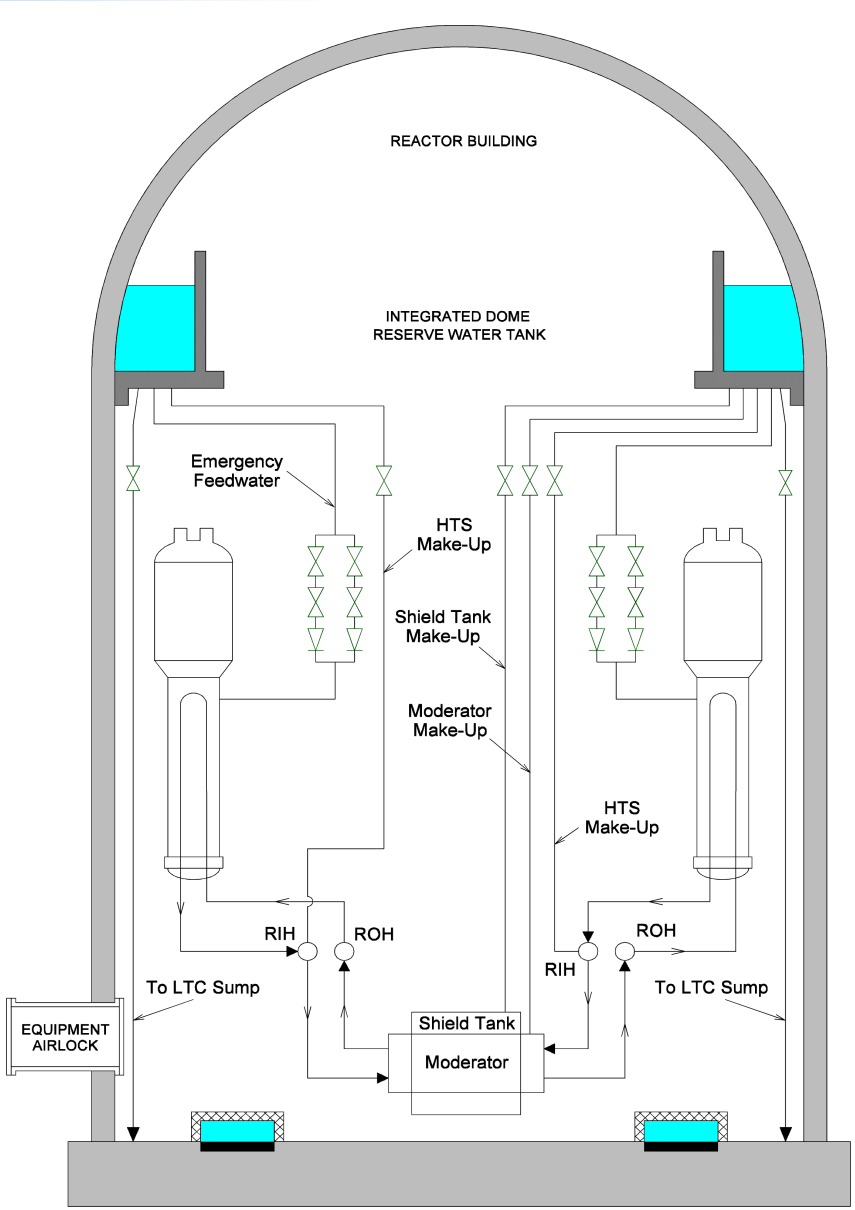
Safety Support Systems

- Reserve Water System
- Cooling Water Systems
- Electrical Power Systems
- Instrument Air Systems
- Secondary Control Building

Reserve Water System

- Large water volume tank at high elevation in the reactor building
- Passive supply of water by gravity for
  - Containment sumps for NPSH of LTC pumps
  - Emergency feedwater to steam generators
  - Emergency make-up to the RCS
  - Make-up to moderator and shield tank for enhanced mitigation of severe accidents

Reserve Water System



In this figure

HTS=RCS

Service Water and Electrical Power Systems

- The systems supply cooling water (raw service water and recirculated cooling water) and electrical power to safety related loads required for transient and accident conditions
- Seismic qualification of service water and electrical power supplies
- Two redundant divisions of service water supplies for safe shutdown of each unit
- Two redundant divisions of Class I, II and III electrical power supplies in each unit
- Interconnection of service water and electrical power supplies between twin units to increase overall reliability and protection against common cause events in either unit

Instrument Air Systems and Secondary Control Building

- Instrument air is provided by compressed air supplies backed up by local air tanks
- Secondary control building completely separate from the main control room provides controls for safe shutdown, cooldown and monitoring of either unit's reactor in case the main control room becomes uninhabitable

Severe Accident Resistance

- Presence of large separate volumes of water in and around the core
- Moderator backup heat sink maintains core coolability in the event of a LOCA combined with the unavailability of the emergency core cooling
- If even moderator cooling is unavailable, the passive thermal capacities of moderator mass inside the calandria and light water in the shield tank slow down the progression of severe core damage
- Hence, a more benign (slower) challenge to the containment boundary with more time for recovery actions
- Further enhancements in ACR with the provision of passive water makeup to moderator and shield tank from the reserve water system to extend their passive thermal capacities

Heat Sinks for Severe Core Damage (SCD) Prevention and Mitigation

SCD Prevention (no loss of core coolability)

- **Normal Heat Removal Systems**
- **Emergency Heat Removal Systems**
  - **–Emergency Core Cooling**
  - **–Passive Emergency Feedwater from Reserve Water Tank**
- **Backup moderator heat sink**

SCD Mitigation

- **Passive thermal capacity of moderator**
- **Passive thermal capacity of shield water**
- **Passive makeup to calandria vessel and shield tank from Reserve Water Tank**
- **Severe Accident Management**

Conclusion

- Enhanced inherent safety characteristics compared to existing CANDU plants
  - Negative power reactivity coefficient
  - Small negative void reactivity coefficient giving more balanced nuclear protection between LOCAs and fast cooldown accidents
  - Larger thermal margins due to the use of CANFLEX fuel
- Enhanced engineered safety features
  - ECI system simplification
  - Reserve Water System for severe accident prevention and mitigation
  - Steel-lined, single-unit containment structure


AECL
TECHNOLOGIES INC.