ACR Guidelines on Safety Design Requirements

By Hardev Johal
Section Head, Safety Design, ACR Development
Presented to US Nuclear Regulatory Commission
Washington DC
March 27, 2003

AECL TECHNOLOGIES INC.

Introduction

- AECL high-level safety requirements for safety related systems
- AECL requirements on Seismic Qualification, Environmental Qualification, Separation of Systems and Components, Fire Protection, Containment, and Radiation Protection
- This presentation introduces these requirements
- In addition, CNSC imposes requirements on safety systems

Requirements on Safety Related Systems

- Safety requirements for safety related systems/structures are identified.
- Systems / Structures
  - Safety Related System/Structure:

    Any system or structure that directly or indirectly performs the safety functions (Shutdown, Fuel Cooling, Confinement of Radioactive Material, Monitor of plant condition).
  - Safety Systems:

    Systems provided specifically to mitigate accident conditions immediately after a failure that could potentially cause a significant release, i.e. SDS1, SDS2, ECCS, containment.
  - Safety Support Systems:

    Systems that provide support services to the Safety Systems (essential to performing the safety functions).

Examples of Safety Requirements

1. Reactor Building

Safety Function:

- Barrier to the release of radioactive materials following a release within the containment envelope.
- Protection of safety related systems from environmental conditions and severe events occurring outside the reactor building.
- Support of safety related systems inside the reactor building (internal structures).

Safety Requirements:

- The reactor building shall be designed with a leak rate which will satisfy public dose criteria for events involving releases of radioactive materials inside the building.

Examples of Safety Requirements - cont.

- The reactor building shall be designed for an internal highest pressure and temperature caused by a loss of coolant accident.
- The reactor building shall retain its structural integrity for main steam line break inside containment.
- The reactor building 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 shall be satisfied.

Examples of Safety Requirements - cont.

2. Reactor Coolant System (RCS)

Safety Function

- Maintain the capability to remove heat from the fuel, including via thermosyphoning.
- During normal operation, provide a barrier to the release of radioactive materials to ensure that doses to plant staff remain within acceptable limits.

Safety Requirements:

- For normal operation and accident events in which the reactor coolant system pressure boundary remains intact, the system shall be capable of removing the stored and decay heat to prevent fuel failures.

Examples of Safety Requirements - cont.

- For events in which the reactor coolant system pressure boundary fails, the system shall, in conjunction with the mitigating systems such as emergency core cooling (emergency coolant injection + long-term cooling), limit the fuel damage to satisfy the regulatory criteria.
- The reactor coolant system pressure boundary shall be designed to withstand the forces and vibration resulting from continued reactor coolant 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.
- The design shall, in conjunction with the emergency core cooling system, satisfy the requirements of CNSC Regulatory Document R-9.

Seismic Requirements

- Seismic design objectives, including seismic level, and safety function to be qualified are identified. Essential systems/structures to be qualified are included.
- Seismic Design Objectives
  - **Sufficient capability to perform the four safety functions (Shutdown, Fuel Cooling, Containment, Monitoring).**
- Seismic Level
  - **Design Basis Earthquake (DBE): engineering representation of the potentially severe effects of earthquakes applicable to the site that have sufficiently low probability of being exceeded, during the lifetime of the plant**

Seismic Requirements

Major Seismically qualified Functions/Systems

- Shutdown Capability
  - Shutdown System 1 (SDS1)
  - Shutdown System 2 (SDS2)
- Fuel Cooling Capability
  - RCS: thermosyphoning.
  - ECI: coolant make-up to cater for small leaks existing prior to a DBE.
  - LTC: long term cooling of the fuel.
  - RWS: Reserve water system supply to RCS, Steam Generators (SGs), Moderator System, LTC and Shield Tank.
  - Main Steam: to ensure that the residual and decay heat can be discharged to the atmosphere.
  - Service Support Systems (Service Water Systems, Electrical Power Supply and Instrument Air Supply): qualified to support operation of mitigating systems.

Seismic Requirements

- Containment Capability
  - Containment
  - Isolation
  - Local air coolers
  - Hydrogen control
- Control and Monitoring Capability
  - Main Control Room
  - Secondary Control Building

Seismic Requirements - Examples

Seismic Requirements for Reactor Building:

- **All components that make up the containment boundary shall maintain their structural integrity during and following a DBE so as not to compromise safety related systems.**
- **The design shall comply with CAN3-N287.3, "Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants". All internal structures, major equipment supports and shielding structures shall be qualified to retain structural integrity and/or load bearing capability.**
- **The containment boundary includes all those sections of piping systems, ducts and cable seals within the reactor building which penetrate the containment structure. Refer to CNSC document R-7 "Requirements for Containment Systems for CANDU Nuclear Power Plants".**

Seismic Requirements - Examples

Seismic Requirements for Reactor Coolant System:

- The reactor coolant circulating pumps shall remain free wheeling and the reactor coolant system shall be qualified (Service Level C) to retain its natural circulation capabilities during and following a DBE.
- The steam generator shall be qualified so it will remain a heat sink following a DBE. The steam generator secondary side water shall not drain. The feedwater piping and check valves inside the reactor building shall be qualified.
- All the subsystems directly connected to the main circuit shall be qualified to DBE to ensure pressure boundary integrity of the RCS or be isolatable.
- All equipment necessary to support thermosyphoning shall be supplied with qualified power if necessary to maintain adequate inventory in the core.
- RCS instrumentation associated with Post Accident Management (PAM) shall be seismically qualified.

Environmental Qualification

- Requirements for EQ program, environmental conditions, and systems performing safety functions are identified.
- Aspects of Environmental Qualification Program:
  - Events causing harsh environmental conditions are identified.
  - Essential systems and components required to perform safety functions during these events are identified.
  - The environmental conditions and their durations, that the component must withstand during normal plant operation and during the course of the accident are identified.
  - The safety function, the performance requirements, and the mission time are identified for the components requiring environmental qualification.
  - The components to be environmentally qualified are tested or analyzed to demonstrate that they will perform their required safety functions during the harsh environmental conditions.
  - Requirements for maintaining the qualification of the required components during construction and operation of the plant are identified.

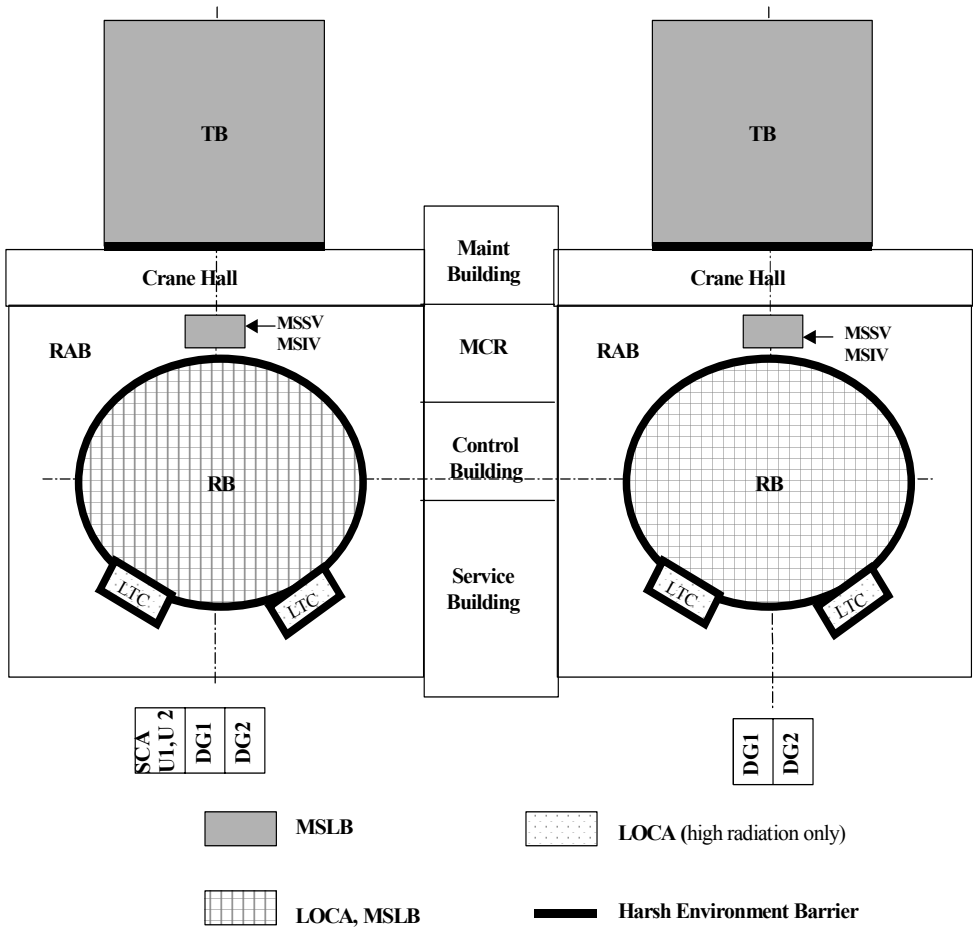
Environmental Qualification

Identification of systems and components requiring EQ

- **Systems credited in safety analysis (shutdown, heat removal, containment and monitoring) are qualified for applicable accidents.**

Environmental Qualification

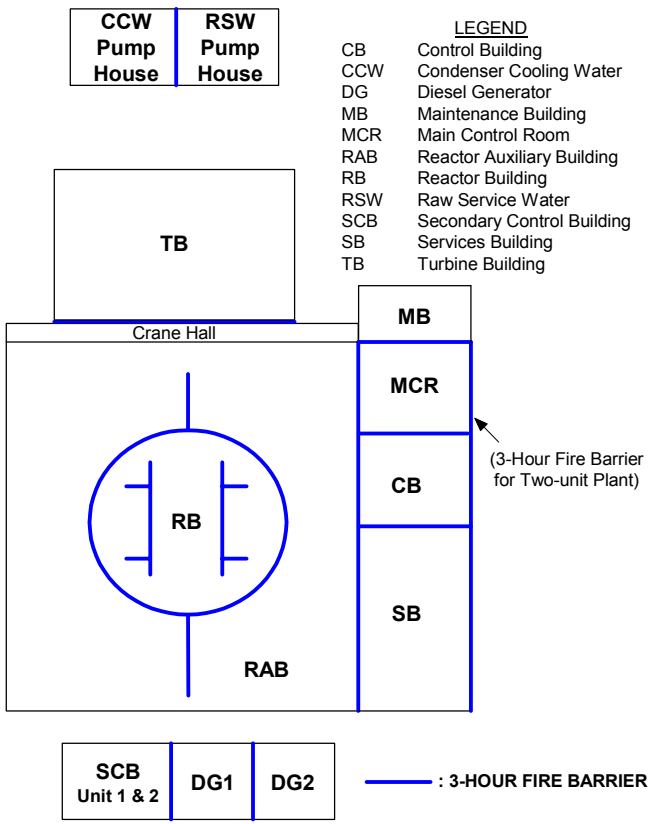
Plant Areas Subject to Harsh Environment (Conceptual Schematic)



Separation of Systems and Components

- Separation requirements for systems are identified so that essential safety functions can be performed for common cause events.
- Separation features provide protection against common cause events. No more than one of two redundant safety systems and no more than one of two divisions within a safety system or a safety support system would be disabled by a common cause event.
- Common Cause Events
  - External to Reactor Building
    - Earthquake, fire, missiles, flood, adverse environment
    - Extreme External Events (e.g., tornado, aircraft crash)
  - Internal to Reactor Building
    - Earthquake, fire, missiles, flooding.

External Events Protection



Redundant Divisions

- Divisions of the system are designed to be independent of the other, to the maximum extent practical. Examples of systems having divisions are:
  - Recirculating Cooling Water System
  - Raw Service Water System
  - Long Term Cooling System
  - Electrical Power Distribution

Channel Designation and Separation

Major Safety Related Systems	Channel Routing and Identification		
Reactor Regulating System, Control and Process Systems *	A	B	C
Shutdown System #1*	D	E	F
Ventilation Isolation System *	NN	PP	QQ
Emergency Coolant Injection System *	K	L	M
Long Term Cooling System *	KK	LL	MM
Shutdown System #2 **	G	H	J
Containment System **	N	P	Q
Second Crash Cooldown System **	X	Y	Z
Reserve Water System, Post Accident Monitoring (dedicated) **	R	S	T
Electrical System	ODD	THIRD	EVEN

Summary of Separation Requirements

TYPE OF SEPARATION	Minimum Requirement
Outside Reactor Building: Other Connected Building	**Barriers/Fire Walls (3-hour barrier or 6 m distance)**
Both Inside and Outside Reactor Building	
1. Systems	
• Fire Hazard	6 m H/V or Fire Barrier
• Other Hazard	2 m H/V
• No identified Hazards	1 m H/V
2. Instrumentation	
• Triplicated Channels (same system)	2 m except 6 m for fire
• Between banks of trays	0.5 m H/V
• Between Power and Control cable	0.5 m with Power cable on top, or 2 m below
• Between Tubing Routes	0.5 m H/V

Fire Protection Requirements

- Implements requirements of CSA Standard CAN/CSA-N293, “Fire Protection of CANDU Nuclear Power Plants” and IAEA Safety Guides, 50-SG-D2, “Fire Protection in Nuclear Power Plants”.

Safety Criteria for Fire Protection

- Maintain adequate capability to perform the safety functions of shutdown and heat removal, including support services.
- Maintain containment boundary
- Maintain availability of a control area

Requirements for Fire Protection

- Fire protection is addressed in terms of:
  - fire prevention,
  - fire detection and suppression,
  - mitigation of the effects of fires.

Fire Prevention

The potential for fires minimized by:

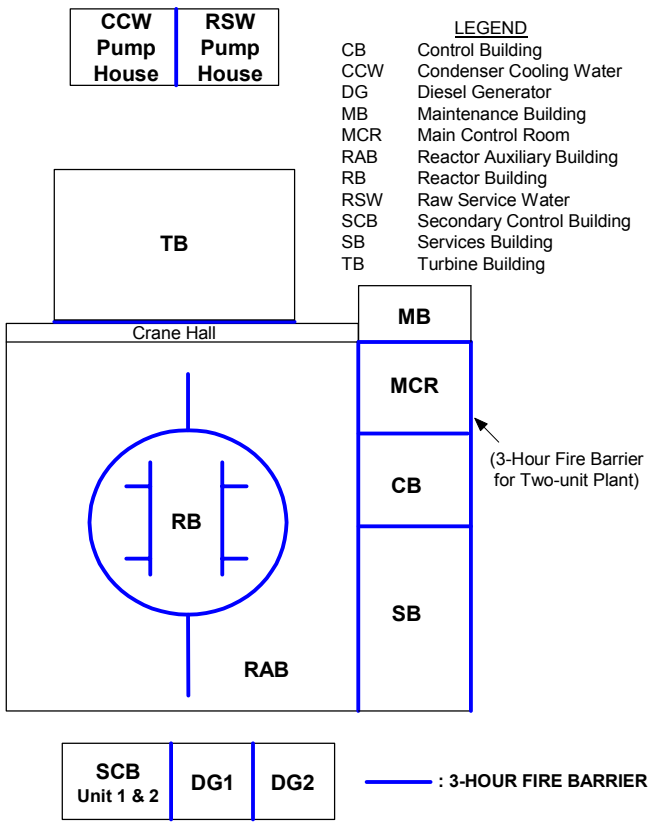
- limiting the use of combustible materials,
- preventing the ignition of combustibles.

Requirements for Fire Protection

Fire Detection and Suppression

- **Detection**
  - Provide fire detection and alarms to bring early operator response, fire suppression, evacuation or other mitigating actions.
  - Consider physical obstructions, ventilation flow and the characteristics of the products of combustion.
- **Suppression**
  - Fire suppression is provided to cope with fire hazards identified in the fire hazards assessment.

Major Fire Barrier Locations (Conceptual Schematic)



Fire Hazards Assessment (FHA)

- A Fire Hazard Assessment is prepared during the plant design, it is used in the design of the fire protection systems for PRA for fire events, and for fire protection planning in the operating plant. Preliminary FHA will be done this year and final FHA after design is complete.
- The FHA Consists of following elements:
  - Area by area data relevant to the assessment
  - Postulation of fires
  - Evaluation of the consequences of fires
  - Fire PRA will be prepared for ACR
- Fire PRA will be prepared for ACR

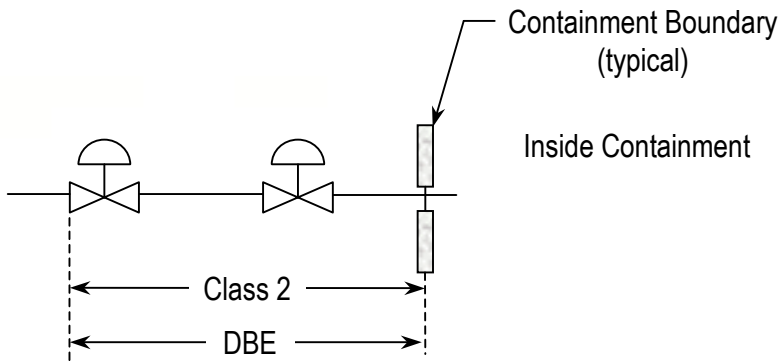
Containment Requirements

- Specifies containment system requirements to implement CNSC R7.
- Containment system includes reactor building (RB), containment penetrations, RB air cooling, RB isolation, hydrogen recombiners.
- ACR provides fast isolation, on high radioactivity or high pressure, of system penetrations that are open to containment atmosphere.

Isolation Requirements of Containment Extensions - Examples

Systems connected to the containment atmosphere

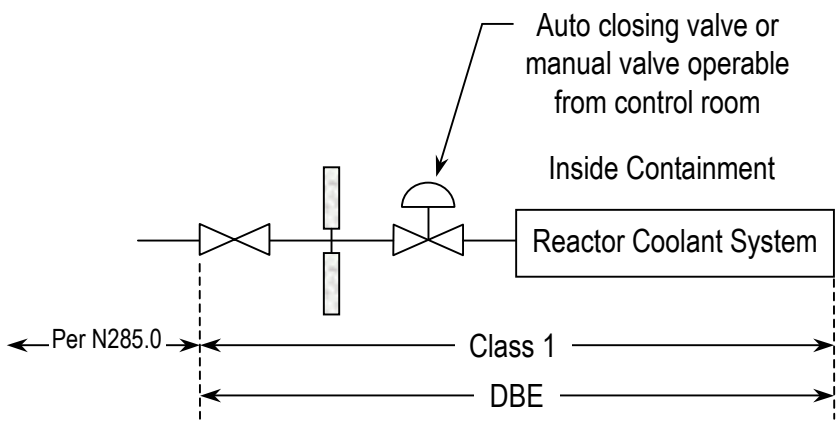
- **Two automatically closing Class 2 isolation valves, one of which may be a check valve, for lines that may be open to the containment atmosphere**

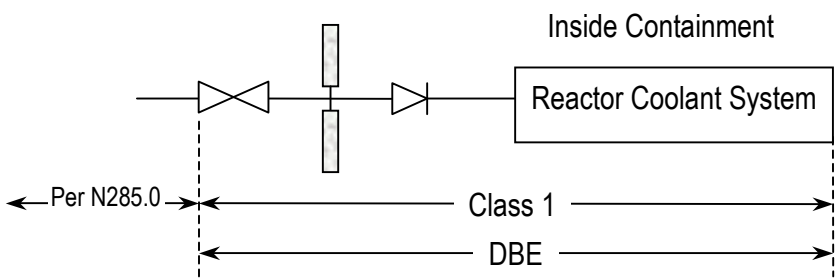


Isolation Requirements of Containment Extensions - Examples

Systems Connected to the Reactor Coolant System

- **Systems having normally open lines shall be provided with two isolation valves, Class 1, one of which can be manually closed from the control room or is automatically closed. A check valve located inside the containment structure is an acceptable automatically closing valve.**





Radiation Protection Requirements

Radiation Protection Philosophy:

- Meet regulatory requirements for the radiation exposure of the public and plant staff
- Radiation exposures during normal plant operation are As Low As Reasonably Achievable (ALARA), social and economic factors being taken into account,
- ACR target: average total station staff exposures 1 person-Sv/a over operating life of a single unit.

Regulatory Limits and Dose Limits

Whole Body Radiation Dose Limits for Normal Operation

Person	Period	Effective Dose (mSv/a)
Nuclear Energy Worker	One year dosimetry period	20
A person who is not a Nuclear Energy Worker	One calendar year	1

Dose and Release Limits for Postulated Accidents

For design purposes, the dose limit (accumulated dose for a NEW over a 90-day period following an accident) is less than 50 mSv in an area of continuous occupancy.

Radiation Protection Design Requirements

Access Control:

- Access control requirements for hazardous areas are given.

Contamination Control

- Design Targets for Control of Tritium are provided.
- Station areas are classified into four zones according to the levels of potential or actual contamination.
- Ventilation system maintains a flow pattern from low to high contamination areas.

Radiation Protection Design Requirements

- ZONE 0: Normally free from contamination but contaminated equipment may move through it (e.g., yard area, pump house). Eating permitted in designated areas.
- ZONE 1: No radioactive equipment, free from contamination. Eating permitted in designated areas (e.g., administration and engineering offices).
- ZONE 2: No radioactive equipment, normally free from contamination; radioactive material from Zone 3 can temporarily create contamination (e.g., reactor auxiliary building and turbine building).
- ZONE 3: contains radioactive material/equipment and presence of contamination should be expected; sources of contamination localized and under control (e.g., reactor building and parts of reactor auxiliary building).

Radiation Protection Design Requirements

- Shielding requirements to reduce dose rates are provided.
- Post accident habitability identifies those areas of the station where access is required after an accident.
- Radiation Monitoring requirements for normal operation and accidents are specified.

Conclusions

- This presentation provided introduction to key areas of the ACR safety requirements
- Detailed system level safety requirements are provided in system design documents


AECL
TECHNOLOGIES INC.