Safety Systems and Safety Analysis of the Qinshan Phase III CANDU Nuclear Power Plant

by

Cai Jianping*, Shen Sen* and Nick Barkman**
*Shanghai Nuclear Engineering Design & Research Institute
** Atomic Energy Of Canada Limited

Introduction

In the safety design for the Qinshan CANDU 6 Nuclear Power Plant, four fundamental safety functions are considered, consistent with international reactor design principles and with the fundamental requirements of the Chinese Code on Nuclear Power Plant Safety Design, HAF 0200 (Reference 1). These four fundamental safety functions are:

- To shutdown the reactor and maintain it in a safe shutdown condition,
- To remove decay heat from the fuel effectively,
- To maintain a barrier to limit radioactive release to the public and plant personnel, and
- To supply information necessary for the operator to monitor the status of the plant.

Nuclear Safety Principles

Safety related systems and structures are defined as those which, by virtue of failure to perform the safety functions in accordance with the design intent, could cause the regulatory dose limits for the plant to be exceeded, in the absence of mitigating system action. Systems that are specifically incorporated into the plant to mitigate the consequences of process system failures are referred to as special safety systems. The four special safety systems in the CANDU design are Shutdown Systems No. 1 and 2 (SDS1, SDS2), Emergency Core Cooling System (ECCS), and containment. Other systems that provide safety related services, such as electrical power, cooling water, and air supplies to the special safety systems are referred to as safety support systems.

The design concepts that ensure that safety systems and safety support systems perform their safety functions with a high degree of reliability, include the use of redundancy, diversity, separation, equipment qualification, quality assurance, and the use of appropriate design codes and standards.

Redundancy is the use of two or more components or systems, each of which is capable of performing the necessary function. Redundancy provides protection against independent equipment failures. Safety design bases for the four special safety systems include the requirement that they be readily testable during plant operation to show an unavailability of less that 10^{-3}.

Diversity is the use of two physically or functionally different means of performing the same function. Diversity provides protection against certain types of common mode failures. Where practical, the special safety systems use diversity in performing the same safety function. For example, the two shutdown systems use different methods of operation and are of a physically different design.

Separation refers to the use of barriers and/or distance to separate components or systems performing similar functions, so that a failure or localized event occurring in or near one system or component is unlikely to affect the other. Separation provides protection against common mode or cross–linked effects, such as fires and missiles. To guard against cross–linked and common mode events, systems are assigned to one of two groups (Group 1 and Group 2). The systems of each group are capable of shutting down the reactor, maintaining cooling of the fuel, and providing plant monitoring capability in the event that the other group of systems is unavailable. The Group 2 systems have the role of mitigating the effects of postulated accidents or external events. Group 1 systems are those primarily dedicated to normal plant power production. The Group 1 and Group 2 systems are located, to the greatest extent possible, in separate areas. Design requirements also specify that the special safety systems be separate from each other and from the process systems to the maximum extent possible.

Safety related systems, structures and components are required to be environmentally and seismically qualified to the extent required for performance of their functions. Qualification ensures that the system, component, or structure can withstand the effects of the postulated earthquake or environmental condition.

A comprehensive quality assurance program is applied to the various stages of design, manufacture, installation, construction, and commissioning of safety related systems, structures and components.

Special Safety Systems

Special safety systems are those systems designed to quickly shutdown the reactor, remove decay heat, and limit the radioactivity release following a postulated failure of a normally operating system. The four special safety systems are Shutdown System No. 1 (SDS1), Shutdown System No. 2 (SDS2), the Emergency Core Cooling System (ECCS), and the containment system. Safety Support Systems are those that provide services needed for proper operation of the Special Safety Systems (e.g., electrical power, cooling

water, instrument air). SDS1 and the ECC system are allocated to Group 1, and SDS2 and the Containment System are allocated to Group 2.

The design requirements for the special safety systems have been formalized in AECB Regulatory Documents R-7 (Containment Systems), R–8 (Shutdown Systems), and R–9 (Emergency Core Cooling Systems), (References 2, 3 and 4). The requirements common to special safety systems include the following:

- Seismic qualification,
- Environmental qualification,
- Unavailability of less than 10^{-3},
- Fail–safe operation,
- On–line testing without impairing,
- Manual initiation from control room,
- Separation and independence from each other and from process systems.

Each of the four Special Safety Systems are described in the following sections.

Containment System

The containment system (Figure 1) is an envelope around the nuclear components of the heat transport system where failure of these components could result in the release of a significant amount of radioactivity to the public. The containment system consists of a post–tensioned pre-stressed concrete containment structure with an epoxy liner, energy sinks consisting of an automatically initiated dousing system and building air coolers, access airlocks, hydrogen control system, and a containment isolation system consisting of valves and dampers in the system lines penetrating containment. Because of the large amounts of energy stored in the heat transport system, the envelope must withstand a pressure rise. The criterion for determining the effectiveness of the envelope is the integrated leak rate for the period of the pressure excursion. To meet the design leakage requirements two diverse principles are used. The first involves design of the envelope to minimize the leak rate. The envelope comprises a primary containment, and a system to automatically isolate the reactor building after a loss–of–coolant accident. The second method involves a system that will absorb the energy released to the envelope, thus reducing the peak pressure and the duration of the pressure excursion. This energy absorbing system is composed of a source of dousing water, spray headers and initiating valves. Reactor building air coolers also help minimize containment leakage by removing energy.

The containment system prevents releases of significant amounts of radioactivity to the public in the event of failure of the nuclear components of the heat transport system.

The design basis event considered is any LOCA event concurrent with complete dousing failure. This event presents the highest potential in terms of peak pressure. However, the

events related to steam systems breaks are also considered in terms of maintaining structural integrity of containment.

Emergency Core Cooling System

The emergency core cooling system (Figure 2) is designed to supply water to the reactor core to provide an alternate means of cooling of the reactor fuel in the event of a loss–of–coolant accident. The emergency core cooling system supplies emergency coolant to the reactor in three stages. The high pressure stage uses gas pressure to inject water into the reactor core from water tanks. The medium pressure stage supplies water from the dousing tank to the reactor core using an emergency core cooling pump. When this water supply is depleted, the low pressure stage recovers the water from the reactor building floor and pumps it back into the reactor core. Heat exchangers cooled by recirculated water (RCW) provide a heat sink for the long-term recovery injection. The emergency core cooling system is initiated automatically on a loss–of–coolant accident signal.

Shutdown Systems No. 1 (SDS1) and No. 2 (SDS2)

Two independent reactor safety shutdown systems are provided. Each shutdown system, acting alone, is designed to shut the reactor down and maintain it in a safe shutdown condition. The shutdown systems are independent of the reactor regulating system and are also independent of each other. Reactor operation is terminated when a neutronic or process parameter enters an unacceptable range. The measurement of each parameter is triplicated and the system is initiated when any two out of the three trip channels are tripped by any parameter or combination of parameters. Provision of two shutdown systems in CANDU means that postulated events coincident with failure of shutdown are incredible, and consequently beyond the design basis.

The first shutdown system, SDS1, consists of shutoff rods, which drop into the core by gravity (assisted by spring force) on receipt of a shutdown signal from the special safety system. SDS1 quickly terminates reactor power operation and maintains the reactor in a safe shutdown condition by releasing 28 spring-assisted shutoff rods into the reactor core. The system has sufficient speed and negative reactivity depth to reduce the reactor power to levels consistent with available cooling.

The design basis events for SDS1 are:

- Loss of regulation,
- Loss of coolant accidents,
- Loss of coolant flow (Loss of Class IV power),
- Loss of secondary side heat sinks,
- Loss of moderator cooling.

With the exception of large loss of coolant accident, for any of these initiating events SDS1 must prevent systematic fuel failure in the reactor.

SDS2 provides a second independent method of quickly terminating reactor power operation by injecting a strong neutron absorbing solution (gadolinium nitrate) into the moderator when any two out of three trip channels are tripped by any parameter or combination of parameters. As far as practicable, the parameters chosen are different from those used for SDS1.

Safety Support Systems

Safety support systems supply reliable services to support the operation of the special safety systems. The Emergency Water Supply System (EWS) provides cooling water to the ECC heat exchangers and make-up water to each primary heat transport system loop and steam generator to ensure fuel cooling after events which cause loss of the normally operating systems, or to act as a backup source of cooling water in the long term after an event. EWS is seismically to during and after an earthquake. EWS is classified as Group 2 and separated from Group 1 systems to provide backup feedwater to the steam generators and backup cooling to the ECC heat exchangers for heat removal from the heat transport system during accident conditions and to provide inventory makeup to the heat transport system via ECC System during accident conditions. The Emergency Power Supply System (EPS) provides the power capability for long–term decay heat removal and for Group 2 post–accident monitoring. EPS is a Group 2 system and meets the two–group separation requirements. EPS provides emergency backup power for a loss of Group 1 electrical in one or both units, a LOCA in one unit followed by SDE 24 hours later, or a Design Basis Earthquake (DBE). EPS is designed to withstand a design basis earthquake and protected against a design basis tornado. Other safety support systems include the Service Water Systems, Instrument Air System, and the Group 1 Electrical Power Supply Systems.

Assessment of Safety System Performance

The nuclear safety principles applied to the design of the CANDU reactors include the assurance that public health and safety are protected even if an accident mitigating system is impaired or unavailable. Therefore, two classes of accidents are defined: a single failure in any of the process systems (those systems required for normal operation), and a single failure in combination with assumed impairments of one of the special safety systems. The combination of a single process system failure, such as a LOCA, together with impairments of one special safety systems, such as the ECCS, is referred to as a “dual failure” event. Such dual failures, considered as severe accidents beyond the design basis in some reactor designs, are considered within the design basis for CANDU.

A comprehensive safety analysis is performed to demonstrate the effectiveness of the special safety systems in meeting the specified requirements with respect to radiation

dose to the public as well as the requirements for fuel, fuel channel and reactor building integrity. Limits for public dose are set by the regulatory agency for specific postulated initiating events, including those events with assumed safety system impairment. The dose limits are related in general although not explicitly to expected frequency. The comprehensive safety assessment for the Qinshan CANDU NPP is documented in the Safety Analysis Report; however, some summary examples are provided here to demonstrate special safety system performance.

Shutdown System Performance

Shutdown system performance, or trip coverage, is assessed for the spectrum of postulated initiating events to demonstrate that there at least two effective diverse trip parameters for each shutdown system acting independently, such that allowable dose limits are not exceeded. Each shutdown system must detect the initiating event in sufficient time, respond quickly enough to reduce reactor power to levels consistent with available fuel cooling, and provide sufficient negative reactivity depth to maintain the reactor in a safe shutdown state.

The limiting event in terms of the ability of the shutdown systems to detect and rapidly shut down the reactor is a large loss-of-coolant accident (LOCA). After a LOCA, there is an increase in coolant void in the reactor core due to depressurization and reduction in coolant flow. In CANDU, increased coolant void leads to a net positive reactivity insertion and hence an increase in power. Each shutdown system design has trip parameters that detect both the power increase and rate of increase, and sufficiently short response time to arrest the power excursion to ensure that fuel channel integrity is maintained. Analysis demonstrates that for the other postulated initiating events, each shutdown system has at least two effective trip parameters to satisfy the safety criteria. Examples include:

Postulated Initiating Event	Effective Trip Parameters (SDS1)	Effective Trip Parameters (SDS2)
Loss of electrical power	High reactor power High heat transport system pressure Low core differential pressure	High reactor power High heat transport system pressure Low core differential pressure
Steam Line Break	Steam generator low level Steam generator feedline low pressure	Steam generator low level Steam generator feedline low pressure
Small loss-of-coolant	Low heat transport system pressure Pressurizer low level	Low heat transport system pressure Pressurizer low level

Emergency Core Cooling System Performance

Following a LOCA, the heat transport system depressurizes. This depressurization of the from operating pressure to the pressure at which ECC water can enter the heat transport system is known as the blowdown phase. It varies in duration from a few seconds for large breaks to several minutes for small breaks. When heat transport pressure measurements indicate that the pressure has dropped below 5.42 MPa(g), the isolation valves between the two heat transport loops are closed, thereby isolating the failed loop from the intact loop. When an independent set of pressure measurements on either loop indicates that the pressure has dropped below the same pressure setpoint, and one of the ECC conditioning signals has been initiated, high reactor building pressure, high moderator level (for in-core LOCA) or sustained heat transport system low pressure (for breaks to small to initiate high building pressure), a LOCA signal is generated and the ECC system is initiated. High pressure injection is enabled at this point by opening the required valves; high pressure injection then begins when heat transport system pressure falls below the pressure in the water tanks. The flow rate from the water tanks is dependent on the break size. The LOCA signal also initiates a rapid cooldown of the steam generators following a time delay of 30 seconds by opening the main steam safety valves (MSSV). This aids heat transport system depressurization, increasing the inject flow.

For the limiting large break loss-of-coolant events, fuel in one pass of the broken loop, can heat up. Some fuel can occur following a large break LOCA. Timely injection of ECC to the broken loop; however, arrests the fuel temperature excursion in time such that the public dose limits are satisfied and that fuel channels remain intact. This is demonstrated by detailed analysis, including specific event simulation with state of the art analytical tools. The analysis models the thermalhydraulic behaviour of the heat transport system during blowdown and subsequent refill, as well as the response of fuel sheath deformation at high temperatures, transport of fission products to determine release from fuel, response of the pressure and calandria tubes, and demonstrates the provision of a long-term heat sink.

Containment System Performance

There are two aspects of demonstrating containment system performance. The first is a demonstration that for all postulated initiating events, the peak containment pressure does not exceed the design pressure. The limiting event with respect to peak pressure is a large loss-of-coolant with an assumed failure of the dousing system. Transient pressure inside the reactor building is predicted by a containment thermalhydraulic code, taking into consideration isolation of containment in response to increased pressure, the energy discharge from the break, the role of heat sinks including building air coolers, and leakage from the building. Peak pressure is shown to be less than containment design pressure for these events.

The second assessment of containment performance is transient analysis of integrated leakage following the relevant postulated initiating events. The objective is to show that releases of radioactivity from containment into the environment are minimized sufficiently so that public dose limits are met. Events considered include large and small loss-of-coolant, including events which affect a single channel and which can lead to fuel failure and activity release from that one channel. Integrated leakage is also performed for loss-of-coolant with an assumed failure of ECC injection. In addition to this dual failure, loss-of-coolant events are assessed with assumed impairments of the various containment subsystems (eg. failure to isolate containment, failure of dousing, deflated airlock door seals, loss of building air coolers). Dose limits are specified for each of the single and dual failure events. Transient analysis of containment response determines the overpressure transient, transport of radionuclides from the break throughout containment and the integrated release from containment. Release paths include the ventilation system in the short time before containment is isolated and leakage, and for certain dual failures containment openings assumed to be impaired. For all events, dose to the public, both individual and population, are shown to be within the regulatory limits.

Summary

The Qinshan CANDU 6 Nuclear Power Plant design includes a set of safety systems that perform the fundamental safety functions of shutting down the reactor, removing heat from the core and limiting release to the public. This is achieved through the principles of redundancy, diversity, reliability, separation, equipment qualification and quality assurance. Analysis of the performance of the special safety systems, as reported in the Safety Analysis Report, shows that the fundamental safety criteria for public dose, and integrity of fuel, channels and the reactor building, are satisfied.

References

1. Regulations on the Nuclear Safety of the People's Republic of China, Regulatory Document HAF 0200, "Code on the Safety of Nuclear Power Plant Design", 1991.

2. AECB Regulatory Document R-7, "Requirement for Containment Systems for CANDU Nuclear Power Plants", February 21, 1991.

3. AECB Regulatory Document R-8, "Requirement for Shutdown Systems for CANDU Nuclear Power Plants", February 21, 1991.

4. AECB Regulatory Document R-9, "Requirement for Emergency Core Cooling Systems for CANDU Nuclear Power Plants", February 21, 1991.

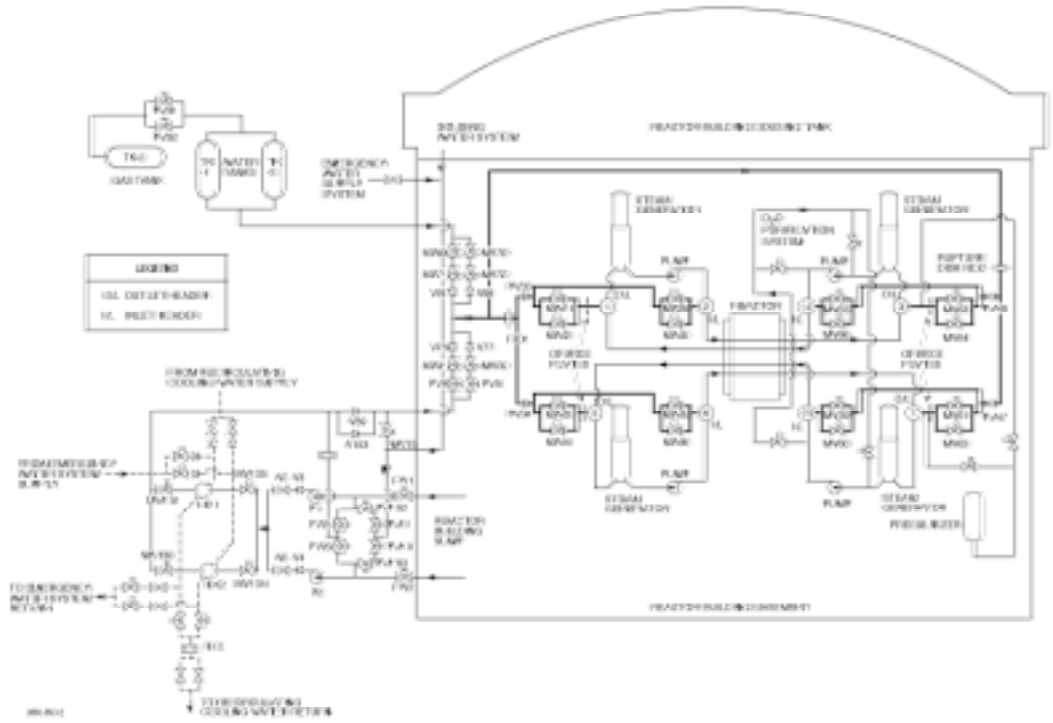

Figure 1: Emergency Core Cooling System

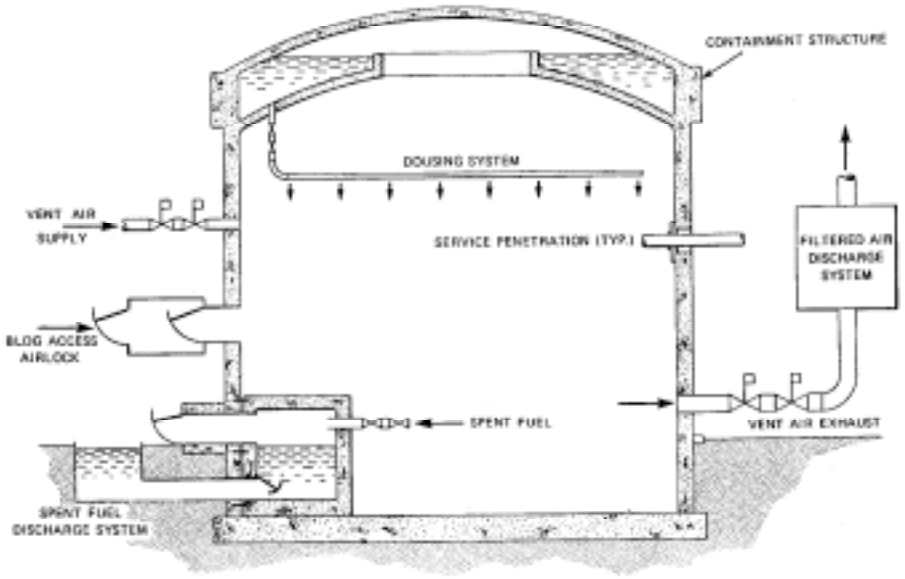

Figure 2 Reactor Containment System