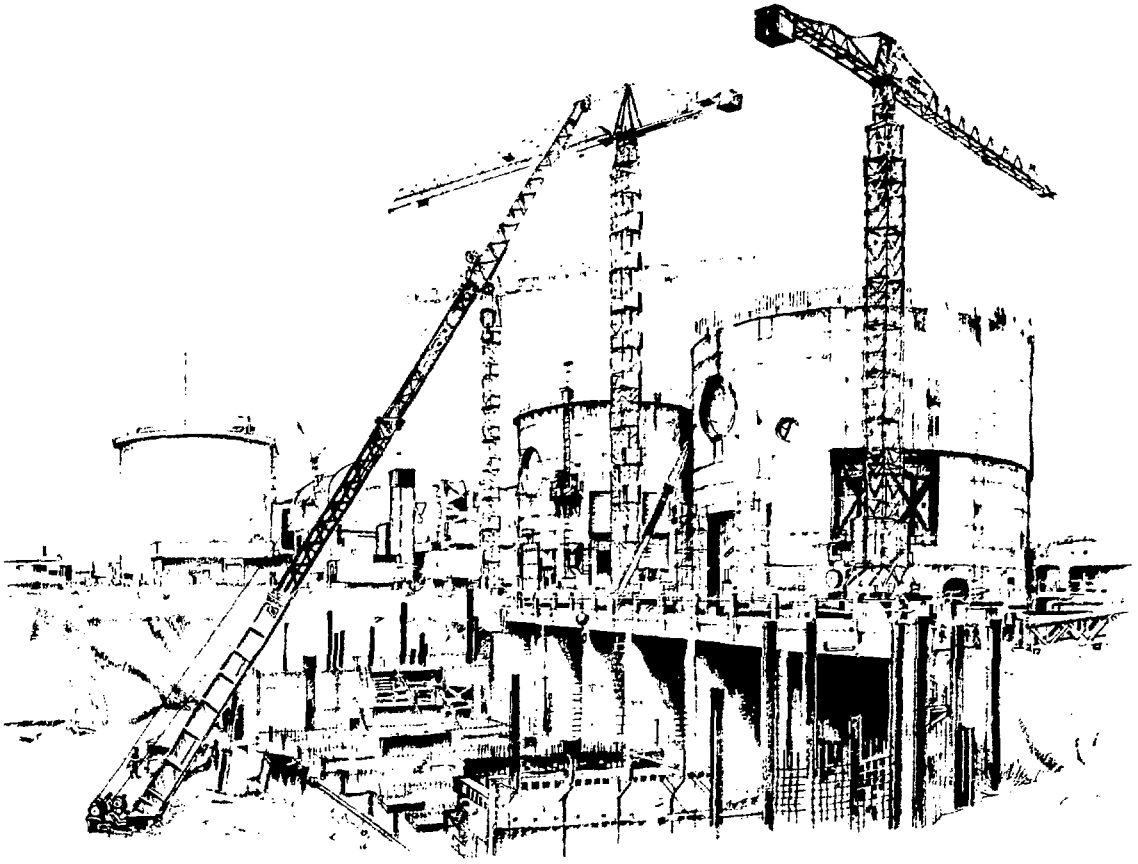
Nuclear Power Reactor Safety

AECL-5694



Atomic Energy of Canada Limited

L'Énergie Atomique du Canada, Limitée

Nuclear Power Reactor Safety

By G. A. Pon

Vice President, Power Projects
Atomic Energy of Canada Limited
Sheridan Park Research Community
Mississauga, Ontario L5K 1B2

October 1976

ABSTRACT

This report is based on the Atomic Energy of Canada Limited submission to the Royal Commission on Electric Power Planning on the safety of CANDU reactors. It discusses normal operating conditions, postulated accident conditions, and safety systems. The release of radioactivity under normal and accident conditions is compared to the limits set by the Atomic Energy Control Regulations.

Ce rapport peut être
obtenu en français sous
le numéro AECL-5694F

Nuclear Power Reactor Safety

by G. A. Pon

1. INTRODUCTION

The nature of nuclear fission is such that our industry has always been one of the most safety conscious. Fission involves the release of large amounts of energy at a high rate accompanied by the production of radioactivity. Furthermore, the introduction of the fission process to the public, in the form of the Hiroshima bomb, has created a fear of the nuclear process which we in the industry have to live down.

2. DEFENCE IN DEPTH

Our basic philosophy in nuclear reactor safety matters is the provision of defence in depth in order to protect the operating staff and the public. We can speak of defence in depth by the identification of three levels:

a) First Level

Design, construct and operate for maximum safety in normal operation and maximum tolerance for system malfunction. Safety begins in the design and is an important factor through all stages of design. This calls for the highest quality in design and materials, a high level of manufacturing inspection, the testing of components and systems, and in-service inspection (see Appendix A). The use of redundant and fail-safe systems ensures further that the system will perform as designed.

b) Second Level

The reactor regulating system controls the reactor and steam raising equipment so that its operating parameters remain within conservative operating limits. It is in operation "full time", and intervenes effectively against many incidents external to itself.

c) Third Level

A third level of protection for the operating staff and the public is provided by reliable safety systems (see Appendix B). These systems are designed to assure that any incidents will be prevented, arrested or accommodated safely. Conservative design practices, adequate design margin, inspectability, and independent redundant detecting and actuating equipment are incorporated in safety systems to ensure effectiveness and reliability. In addition, these systems are routinely monitored and tested so that there is full assurance they will operate when required.

It should be noted also, that substantial margins are included in the design of the safety systems. These ensure further, that if even any one of the safety systems is impaired in some way, or fails to be invoked for whatever reason, the effect on the public remains within Atomic Energy Control Board (AECB) reference levels (Section 6).

3. BARRIERS TO THE RELEASE OF RADIOACTIVITY

In every nuclear power plant there are a number of physical barriers to the release or escape of radioactivity to the public. From the point of view of public safety each barrier forms a back-up system to the others and each is designed, constructed and maintained in accordance with the highest quality standards and engineering principles.

a) The first barrier is the UO_2 fuel. Most of the radioactive fission products are bound within the UO_2 and must diffuse through the fuel if they are to escape. These fission products will not leave the oxide if the sheath fails unless the fuel temperature is raised considerably above the operating level. Even at temperatures near the melting point of UO_2, time is required for the fission products to leave the fuel.

b) The second barrier is provided by the Zircaloy fuel sheaths (thin tubes) into which the UO_2 fuel pellets are packed. The intact Zircaloy sheath will contain any radioactive material that might escape from the UO_2 fuel pellet.

c) The third barrier is the reactor coolant system which consists of piping, pumps, steam generators and other process system equipment. All of these components are built and installed to the highest standards. They are further inspected using the latest techniques during manufacture and in service.

d) The fourth barrier is the reactor building (sometimes called the containment building). This structure is made of reinforced or pre-stressed concrete with walls up to 1.2 m in thickness.

e) The fifth barrier is distance. No permanent habitation is permitted within one kilometre on the land side of the reactor building. The effect is to dilute any radioactivity (which might be released) before it can reach a member of the public.

These barriers are passive in function. They do not need to be triggered to make them work. Their intact physical presence is adequate to satisfy their function.

4. LICENSING

The AECB exercises control over the application and use of atomic energy in Canada. It applies very strict regulatory controls to reactor safety through its licensing process. The formal licensing procedure for a nuclear power plant consists of three steps:

- Site Approval
- Construction Permit
- Operating Licence

a) Site Approval

A site evaluation report is presented to the AECB as the formal document requesting site approval. This document describes the environmental features of the site, e.g. population centres, geology, topography, seismology and meteorology. It includes a brief description of the plant to be built with particular emphasis on the safety systems. Finally, the applicant must show that the criteria for normal and accidental releases of radioactivity will be met.

In Ontario, the utility Ontario Hydro is also holding public meetings to discuss its generating projects. Full site approval by AECB is withheld until these have been concluded. AECB has also indicated its own willingness to hold public meetings if required.

b) Construction Permit

The preliminary safety report is the formal document required for this stage of the licensing process. Sufficient information must be provided on the proposed plant for a comprehensive safety review to be performed. No structural work can start on the site until the construction permit has been issued. The preliminary safety report must be kept up to date by yearly revision.

c) Operating Licence

The issuing of the operating licence implies acceptance by the AECB of the safety aspects of the plant as constructed. Further requirements are that the operating staff must be licensed (by written examination) and the normal and emergency operating procedures approved.

The operating licence covers conditions and restrictions on the release of radioactive effluents from the plant and on allowable modifications to the plant and procedures.

AECB staff are present for all phases of a nuclear power project. The AECB representatives have the authority to examine any aspect of design. During construction, commissioning and early operation of the plant, AECB maintains staff at the site. The AECB receives formal annual reports on operation, radiation exposures and radiation effluents but the staff reviews these matters on a continuing basis.

5. RELEASE OF RADIOACTIVITY DURING NORMAL OPERATION

During normal station operation, minute quantities of radioactivity are released. This aspect of nuclear power is the subject of considerable controversy. It should be noted that man has always lived with radiation. The earth has always been enveloped in radiation from natural sources such as the soil, rocks, minerals, the air and cosmic rays.

The Atomic Energy Control Regulations prescribe the maximum allowable doses of radiation to the public from non-medical uses of atomic energy. The basic limit is 500 mrem per year to the whole body of any individual member of the public and is derived from the recommendations of the International Commission on Radiological Protection (ICRP). Dose limits for specific organs of the body are also stipulated. From the limits on dose, the permissible limits on radioactivity in gaseous and liquid effluents from nuclear power plants are calculated.

Gaseous Releases from the Pickering Station*

	% of Limit				
	1971	1972	1973	1974	1975
Noble Gases	1.7	2.2	1.8	0.20	0.22
Tritium	0.1	0.14	0.33	0.24	0.20
Iodine-131	1.3	0.63	0.025	0.02	0.0045

Liquid Releases from the Pickering Station*

	% of Limit				
	1971	1972	1973	1974	1975
Tritium	0.01	0.016	0.04	0.09	0.064
Gross β/γ	0.12	0.8	0.2	0.29	0.10

* Reference: L.W. Woodhead (Listed in the Bibliography)

Plant operators are required to monitor and control the radioactivity in effluents and to measure doses at the site boundary. Beyond the site boundary, federal and provincial health and environmental agencies conduct a monitoring and sampling program as a further check that the releases are within the limits.

Experience to date has shown that the radioactivity in gaseous and liquid effluents from Canadian nuclear plants has averaged less than a few per cent of the permitted limit.

The tables on the previous page show the good performance to date at the Pickering Nuclear Generating Station.

It is evident that the actual releases are very small relative to the permitted releases and hence the radiation dose received by the public is correspondingly small. The maximum possible theoretical exposure to a member of the public would be obtained by that person who spends 24 hours every day and 365 days in the year standing unsheltered at the plant fence. He could receive a dose of about 5 mrem in a year.

How does this compare with everyday levels of exposure?

Everyone in North America is continuously exposed to about 100 mrem per year. About one third of this comes from cosmic rays, another third from the materials of the house one lives in, a quarter would come from the minerals in the food we eat and the remainder from the ground and the air. The following table compares the annual radiation dose from the various sources.

Radiation Dose from Various Sources – mrem/a

Natural Background	100
Chest X-Ray (1/a)	100-200
Dental X-Ray (1/a)	20
Jet Flight - 10 000 km	4
Luminous Dial Wrist Watch	2
Colour TV (1 h/d)	2
Nuclear Power Plant (maximum exposure plant fence)	5

A general conclusion one may draw from the above tables is that the amount of radioactivity released from Pickering is very small and adds a negligible amount to the radiation by the public from natural and medical sources.

6. RELEASE OF RADIOACTIVITY DURING ACCIDENTS

In accident analyses, we divide the power plant into two types of systems, process systems and safety systems.

Safety systems are - shutdown systems
- emergency core cooling systems
- containment systems

Process systems are the remainder of the plant.

Single failures are defined as a failure in one of the process systems. Dual failures are defined as a failure in a process system coincident with an arbitrary assumed failure of one of the safety systems.

Some examples of single failures are:

- Pipe rupture
- Pump failure
- Electrical supply failure
- Control system failure

Some examples of dual failures are:

- Pipe rupture and shutdown system failure
- Pipe rupture and emergency core cooling system failure
- Control system failure and shutdown system failure

The AECB reference levels for single and dual failures are as follows:

AECB Limits on Exposure

	Single Failure	Dual Failure
Individual		
– Whole Body Exposure	0.5 rem	25 rem
– Thyroid	3.0 rem	250 rem
Population		
– Whole Body Exposure	10^4 man-rem	10^6 man-rem
Maximum Frequency	1 in 3 years	1 in 3000 years

As far as public safety is concerned, Iodine-131 (which is in gaseous form at normal temperatures and pressures) is the most significant isotope during accidental releases. In a 600 MW(e) reactor, the total Iodine-131 inventory is about 10 million curies.*

Now we must translate the rules as given previously for the maximum dose permitted to an individual, to release of Iodine-131 from the containment during an accident.

The releases corresponding to the individual dose limits are as follows:

Derived Limits on Release of Radioactivity

Single Failure	Dual Failure
~10 Curies Iodine-131	~1000 Curies Iodine-131

We therefore must have an attenuation of 10^4 to 10^6 from the total Iodine-131 in the reactor to that released to the public.

Accidents are analyzed pessimistically. For example let us look at some of the assumptions that go into the analyses of the dual accident with pipe rupture and shutdown system failure.

- Pipe is assumed to rupture in any location
- Pipe is assumed to rupture instantaneously and the break area can be as large as twice the cross-sectional area of the pipe
- Atmospheric inversion conditions are assumed
- Light wind is assumed to be blowing in the direction of highest population density

Now, recall that the permitted maximum frequency of this type of incident is once in 3000 years and that the permitted release is about 1000 curies of Iodine-131.

Our analysis for Bruce indicates that the probability of this event occurring is about once in one million reactor years and the release of Iodine is near zero.

A realistic estimate comparing the risks associated with a nuclear power station with the risks of everyday living has been made in a study directed by Dr. N.A. Rasmussen of the Massachusetts Institute of Technology.†

The team of 60 spent three years on the study using the methods developed by the US National Aeronautics and Space Administration for their space program. Although the study was prepared in the US assessing the risks associated with their light water nuclear power plants, the findings should not be significantly different for the CANDU reactor. Some of these findings are:

Probabilities of Major Man-Caused and Natural Events

Type of Event	Probability of 100 or More Fatalities per year	Probability of 1000 or More Fatalities per year
Man-Caused		
Airplane Crash	1 in 2	1 in 2000
Fire	1 in 7	1 in 200
Explosion	1 in 16	1 in 120
Toxic Gas	1 in 100	1 in 1000
Natural		
Tornado	1 in 5	very small
Hurricanes	1 in 5	1 in 25
Earthquake	1 in 20	1 in 50
Meteorite Impact	1 in 100 000	1 in 1 000 000
Nuclear Power		
(100 Plants)	1 in 10 000	1 in 1 000 000

* 1 curie = 37 GBq

† Reference: WASH-1400 (listed in the Bibliography)

BIBLIOGRAPHY

Accident Analyses . . . . . J.D. Sainsbury, Atomic Energy of Canada Limited, Power Projects; Nuclear Energy Symposium, Canadian Nuclear Association/Atomic Energy of Canada Limited, Montreal, 1974

Nuclear Power Safety in Canada . . . . . G.C. Laurence, Atomic Energy Control Board, Ottawa; Report AECB-1058, January 1972

Reactor Licensing and Safety Requirements . . . . . D.G. Hurst and F.C. Boyd, Atomic Energy Control Board; Canadian Nuclear Association 12th Annual Conference, Ottawa, Paper No. 72 - CNA - 102, June 1972

AECL Symposium on Nuclear Energy . . . . . Atomic Energy of Canada Limited, Power Projects Publication PP-24, March 1974

Performance Review of CANDU-PHW Nuclear-Electric Units and the Bruce Heavy Water Plant . . . . . L.W. Woodhead, Ontario Hydro; Joint Canadian Nuclear Association/American Nuclear Society meeting, Toronto, June 1976

PHWR Safety . . . . . L. Pease, Atomic Energy of Canada Limited, and R. Wilson, Ontario Hydro; Joint Canadian Nuclear Association/American Nuclear Society meeting, Toronto, June 1976

Reactor Safety Study . . . . . An assessment of accident risks in US commercial nuclear power plants, US Nuclear Regulatory Commission. Report WASH-1400 and appendices, October 1975

Water Reactor Safety . . . . . Topical Meeting of American Nuclear Society, Salt Lake City, March 1973; Document CONF-730304, published by U.S. Atomic Energy Commission, Technical Information Center, Springfield, Virginia

Principles and Standards of Reactor Safety . . . . . Symposium of International Atomic Energy Agency, Julich, February 1973, IAEA Publication STI/PUB/342

Water-Cooled Reactor Safety . . . . . An assessment prepared for the Committee on Reactor Safety Technology, European Nuclear Energy Agency, OECD, Paris, May 1970

A Criteria Digest on Radioactivity in the Environment . . . . . H.C. Rothschild; NRC Associate Committe on Scientific Criteria for Environmental Quality, National Research Council of Canada, Ottawa, Report NRCC No. 13566, October 1973

Appendix A

PERIODIC INSPECTION

The requirements for the periodic inspection of important reactor system pressure boundaries are spelled out in Canadian Standards Association standard CSA N285-4. The purpose of the inspection is to provide continuing assurance of the in-service integrity of the pressure boundaries of selected reactor systems. This is a safety oriented function. The systems to be inspected are obviously those where failure could lead to releases of radioactivity. They are identified in three categories:

a) Systems containing fluid for the cooling of reactor fuels.

b) Systems essential for the safe cooling of the reactor fuel in the event of a process system failure.

c) Other components whose failure or dislodgment could jeopardize the integrity of systems in groups (a) and (b).

Appendix B

SAFETY SYSTEMS

Safety systems are incorporated into the station to limit radioactive releases to the public for two classes of events:

- A single failure in a process system combined with the coincident unavailability of one of the safety systems (a dual failure)
- A single failure in a process system

These systems are independent in design and have minimal operational connection with any of the process systems.

Station Safety Design Assumptions and Criteria

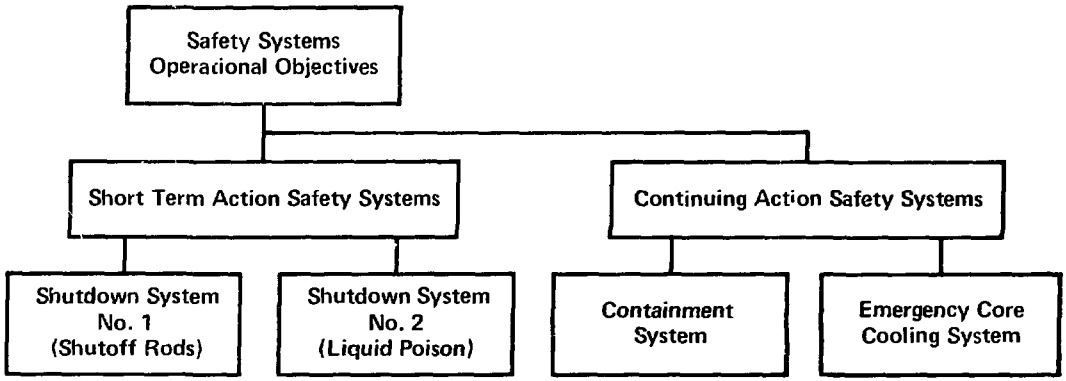
The plant is designed to limit releases of radioactivity to the levels specified in the Atomic Energy Control Board Siting Guide in the event of a process system failure combined with the unavailability of a safety system.

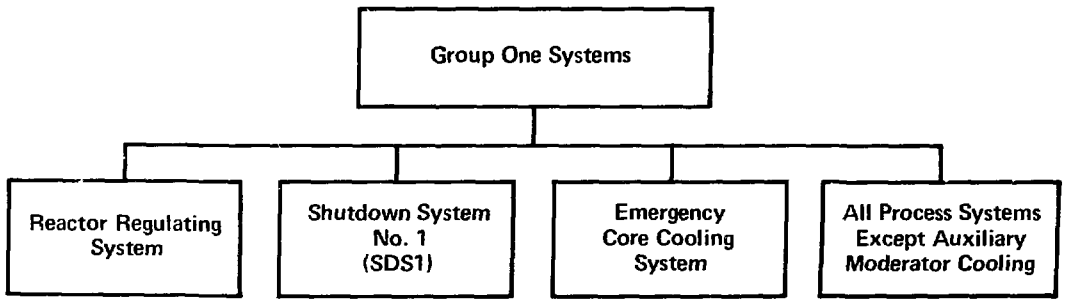
Each safety system is designed for an unavailability of less than 8 hours per year.

The provision of two reactor shutdown systems permits the assumption that at least one will operate following any single process system failure for which both are designed to be effective.

Common Mode Incidents

To protect the plant against 'common mode' incidents such as fires, turbine missiles, and aircraft strikes — although highly improbable — that could affect many safety and safety related systems at the same time, all such systems for future reactors, have been divided into two groups physically separated both inside and outside the building. Each operational group is independently capable of ensuring that the plant is in a safe shutdown state.





Group One Systems and Group Two Systems
The common design requirements for the groups are to:

- Shut down the reactor
- *Remove decay heat from the reactor fuel*
- Supply necessary information to permit the operators to assess the state of the nuclear steam supply system

GROUP ONE SYSTEMS

Reactor shutdown is effected for Group 1 by the Shutdown System No. 1 (SDS1). Decay power is removed by discharge of steam from the steam generators with make-up supplied by the auxiliary feedwater system. In the event of a loss-of-coolant accident, cooling of the failed circuit is provided by the Emergency Core Cooling (ECC) System, with decay power from the failed circuit rejected to the ECC recovery heat exchanger. Decay power from the operational circuit is rejected in the normal fashion via the steam generators.

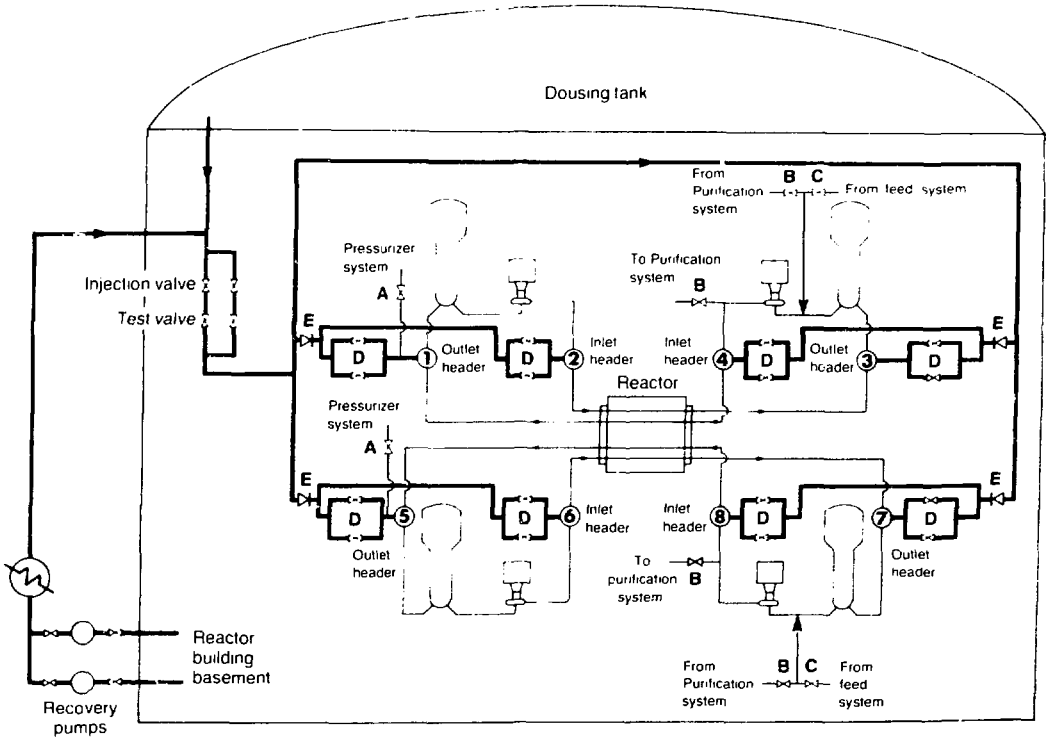
Shutdown System No. 1

The primary method of quickly terminating reactor operation when certain parameters enter an unacceptable range is the release of spring-assisted gravity-drop shut-off rods. Shutdown System No. 1 employs an independent triplicated logic system, which senses the requirement for reactor trip and de-energizes the direct current clutches to release the shut-off rods.

Emergency Core Cooling System

In the event of a loss-of-coolant accident, the pressure inside the Reactor Building rises and a pressure signal is used to close the valves, (A, B, C) in all the interconnection lines joining the heat transport circuits. This action isolates the ruptured from the unruptured circuit.

The heat transport circuits are thus isolated from the pressurizer, feed and purification systems. In addition, the safety relief valves on the steam generators are opened. These provide steam generator rapid cool-down before emergency core cooling commences.



When the pressure in the ruptured circuit has decreased sufficiently the H_2O emergency cooling injection valves and all D_2O emergency cooling valves (D) open. The check valves (E) prevent any outflow of D_2O. The flow of emergency coolant commences when the pressure in the ruptured circuit is less than the pressure due to the static head of water in the dousing tank.

On depletion of the stored water from the dousing tank, core cooling flow is provided by connecting the Reactor Building basement to the recovery pump suction. The mixture of H_2O and D_2O which has been discharged from the break collects in the basement and continues to be re-circulated. The re-circulated flow is cooled to the required injection temperature by the recovery heat exchanger. The water enters the system at a point upstream of the H_2O injection valves to pass over the fuel and discharge out of the break.

GROUP TWO SYSTEMS

Reactor shutdown is effected by Shutdown System No. 2 (SDS2). Activity release is prevented by the Containment System and also by maintaining the other barriers that still exist after an accident. Decay power removal is effected by a supply of emergency water to the steam generators.

Emergency power is provided to act as an alternative source of electrical power for Group Two safety and safety support systems.

Shutdown System No. 2

A second method of quickly terminating reactor operation when certain combinations of very unlikely failures occur, is the rapid injection of concentrated gadolinium nitrate solution into the bulk moderator through horizontally distributed nozzles. This second shutdown system employs an independent triplicated logic system which senses the requirement for this emergency shutdown and opens fast acting helium pressure valves to inject the gadolinium poison into the moderator.

Emergency Power Supply System

The Emergency Power Supply System is provided to supply the necessary power to the Emergency Water Supply System valves and to provide power to the Group Two safety and control systems for operator control of the station from the secondary control area.

Emergency Water Supply System

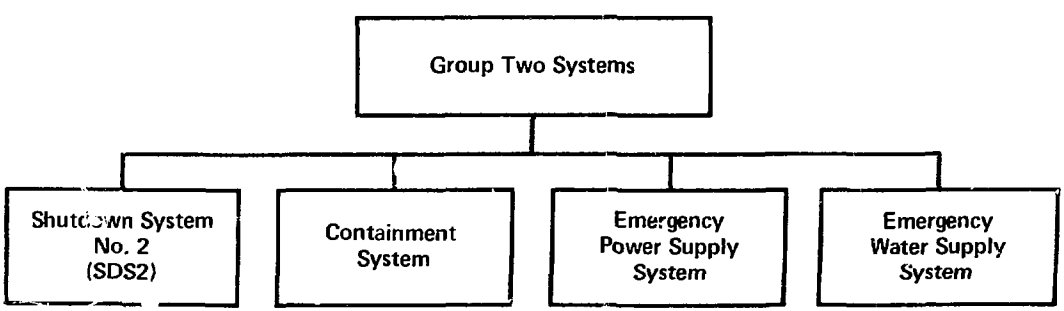
This system is designed to provide an alternative source of water in the unlikely possibility that:

- Make-up water to the heat transport system or steam generators should fail
- Service water to the ECC heat exchanger should fail

Containment System

The Containment System is basically an envelope around the nuclear components of the reactor coolant systems. Failure of these components could result in release of a significant amount of activity to the public. Because of the large amounts of energy stored in the reactor coolant systems, the envelope must withstand a significant 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 approaches are taken:

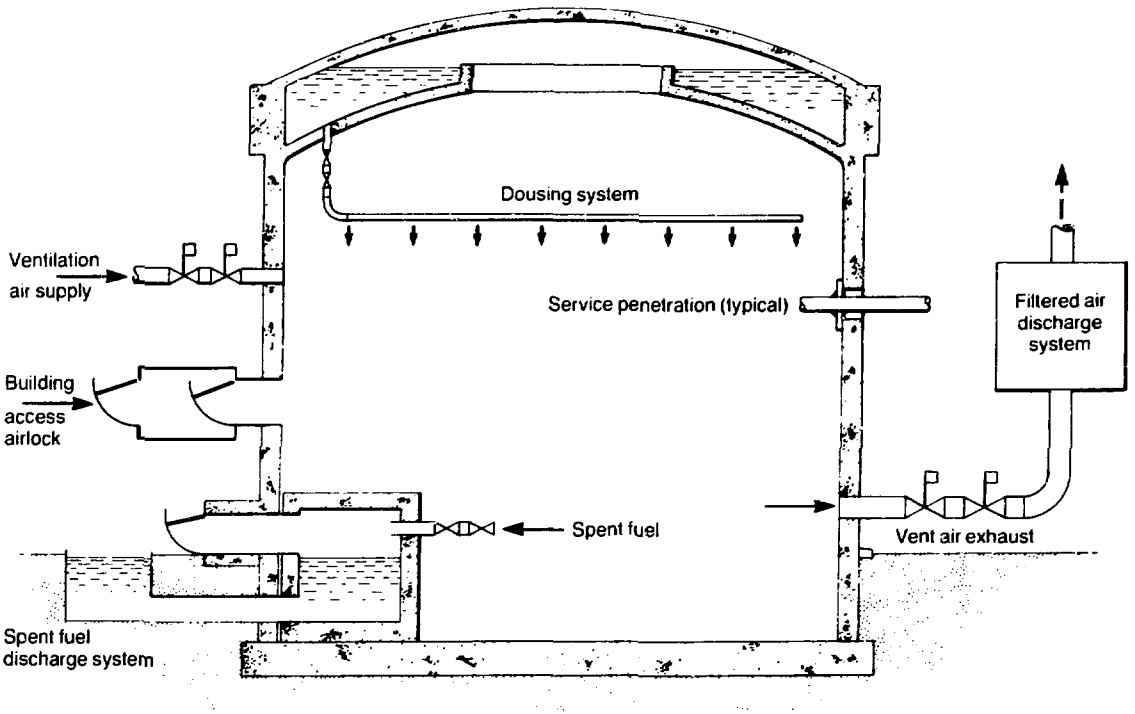
- The first involves the detailed design and testing of the envelope to minimize the leak rate



- *The second involves the addition of a system that* will absorb the energy released to the envelope, thus reducing the peak pressure and the duration of the pressure excursion

The energy absorbing system comprises a source of dousing water, spray headers and initiating valves and building air coolers.

The overall containment system comprises a pre-stressed post-tensioned concrete containment structure with a plastic liner, energy sinks consisting of an automatically initiated dousing system and operational building air coolers, a clean air discharge system, access air locks, and an automatically initiated containment closure system consisting of valves and dampers in system lines open or possibly open to containment during normal operation.



The International Standard Serial Number

ISSN 0067–0367

has been assigned to this series of reports.

To identify individual documents in the series we have assigned an AECL– number.

Please refer to the AECL– number when requesting additional copies of this document from

Scientific Document Distribution Office
Atomic Energy of Canada Limited
Chalk River, Ontario, Canada

K0J 1J0

Price - $2.00 per copy

397-77