CANDU 3 SYSTEMATIC PLANT REVIEW - A NEW APPROACH

R.K. Jaitly and P.J. Allen
AECL CANDU
2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

ABSTRACT

Evaluation of nuclear power plant designs, including the determination of a design basis accident set, is a process that has been evolutionary. As more experience has been gained from the design, operation and licensing of established design concepts, the set of accidents and the range of conditions for evaluation has steadily grown.

Recognition of this evolution has led the Canadian regulatory body, the Atomic Energy Control Board (AECB), to require for all future plants a systematic review (Reference 1) of the plant design. The purpose of this systematic review is to come up with an exhaustive list of design basis accidents. It also gives the reviewer of the design confidence that a systematic, auditable process has been used to derive the list. Accident analysis for each of the events on the list is then used to determine the range of conditions for safe operation of the plant.

The CANDU 3 is the newest design of CANDU nuclear power station. It provides the economy of operation of other CANDUs in a smaller unit size (450MW). A key part of the CANDU 3 design program is a review of the design by the Canadian regulatory prior to the start of construction. These up front licensing discussions provide the first opportunity for the AECB and industry to explore what full implementation of the Systematic Review concept entails. This paper, provides the regulatory background to the Systematic Review, the review process developed by Atomic Energy of Canada Ltd for CANDU 3 and the results of the review. This review process can be applied to any innovative design and provides a framework for identifying all internal events of safety significance. (External events are derived through the site investigation process.)

1. INTRODUCTION

Nuclear regulatory and design organizations throughout the world have a tradition of looking at the response of nuclear power plants to a set of design basis accidents. Ensuring that doses to members of the public and the operating staff are limited for these events has been one important way of making sure that the public is protected. Other safety initiatives include accident prevention and mitigation by quality design, fabrication and construction, inspection, maintenance and testing of components, careful site selection, design of an appropriate operator interface and operator training.

More recently, Probabilistic Safety Assessments (PSAs) have been used to perform analyses to determine the risks arising from plant operation in a more integrated way. The PSAs have proven to be of value in identifying dominant risk contributors and assessing design options to improve safety. One current limitation of the PSA is that it is difficult to be sure that the analyst has identified an appropriate and comprehensive set of initiating events, particularly for innovative designs. Also, PSAs have been slow to gain acceptance as a regulatory tool because the results are very much a function of the methodology employed.

In Canada, there have been several attempts to rationalize the safety assessment process to integrate PSA into the licensing process. The AECB produced a set of draft regulations (Reference 1)in June 1980. These were applied on a trial basis in the licensing of the multi-unit (4x881 MW) Darlington Nuclear Generating Station. With the licensing process for the CANDU 3 design under way, these regulations are being refined to reflect the Darlington experience. The regulatory dose limits to the most exposed public member are shown in Table 1. The proposed frequency ranges shown for the five classes of the events in this table are the proposed guidelines based on Chapter 1 of the Darlington Safety report. [NOTE: The maximum dose, minimum frequency category addressed by the AECB regulations is restricted to a whole body dose limit of 25 rem. The regulations do include a specified list of very low probability events which could result in higher doses. Analysis of these events must be submitted for regulatory evaluation].

A minimum list of abnormal events to be analyzed is given in the AECB consultative document C-6 (Reference 1). The C-6 also requires a systematic review of the plant design to identify all safety significant failures and combination of failures. This paper describes the CANDU 3 Accident Assessment Program which is our proposed response to the C-6 requirements. In more detail, this paper gives the results of the first step in the program which is an exhaustive and systematic review carried out for the CANDU 3 plant design thereby establishing a complete list of initiating events for the probabilistic and consequence analysis.

2. SYSTEMATIC PLANT REVIEW DESCRIPTION

This paper aims to provide an insight into the overall CANDU 3 Accident Assessment Program as shown in Figure 1, with a particular emphasis on the identification of design basis accidents. Main elements of the program are discussed below:

a. Systematic Plant Review for Failure Modes

The objective of the systematic plant review is to identify those abnormal events which potentially constitute public risk to radiation. The review starts by identifying all systems that normally contain significant radionuclide inventories. These are the Heat Transport, the Moderator and the Fuel Handling Systems. Failure of individual and multiple components in these systems are reviewed and the failure modes and their effects listed. The next step is to identify all interfacing systems and any systems that are physically adjacent to the system containing radionuclides. Failures in these systems are then examined to determine if radionuclide release could occur. As a minimum, loss of system function, loss of flow, loss of pressure boundary integrity and loss of heat sink are addressed. It should be noted that failure of all support systems such as electrical power, cooling water, instrument air, HVAC and control systems are included as part of the review of the interfacing systems.

The result of this process was a list of 274 failure modes that could potentially lead to a release of radioactivity.

b. Failure Mode Grouping

The Systematic Plant Review process provides an insight into various failure modes of the systems where the radionuclides normally reside. Subsequently, these failure modes are reviewed for similarities with a view to group failure modes with similar plant response (i.e. requiring same mitigating actions) into a single event. The main objective of this exercise was to combine the 274 failure modes into a smaller, more manageable number of initiating events

for the purpose of analysis. For example, various failure modes relating to the failure of condensate system ultimately lead to a loss of feedwater to the steam generators. Accordingly, failure modes of the condensate and feedwater systems can be conservatively grouped into a single event as "failure of feedwater". In system reliability documents, the fault tree analysis for the loss of feedwater will account for the contribution from the condensate as well as the feedwater systems. It is recognized that the dynamics (i.e., time to loss of normal heat sink) of the plant response for the failures in these two systems may be different due to the stored deaerator storage tank inventory. However, the event tree will assume the fastest of all contributing system failures, and the results will thus be conservative.

The grouping process allowed the 274 failure modes to be combined into 84 initiating events (see Table 2). These grouped events are then used as initiating events for the purpose of event tree analysis.

c. Event Tree Analysis

Plant response to the 84 grouped events is assessed by event tree analysis where the initiating event is credible and the plant response to the event includes multiple mitigating systems. To the extent possible, system interfaces are shown in the tree. Clearly, at an early stage in the design process, accurate evaluation of endpoint frequencies is not possible. However, ball park reliability estimates for the conceptual PSA are derived based on simple fault trees or experience. The CANDU 3 Accident Assessment Program established reliability targets based on the event trees and the desired level of safety (prevention of severe accidents is a key consideration). System reliabilities will be calculated once the design details are available. In addition to independent failures, Common Cause Failures will be addressed in the PSA which is produced at the end of the design program (Generic PSA).

The event trees are also used to identify the systems used to mitigate each accident. This is an important input to the Environmental Qualification and Pipe Whip Assessment.

d. Event Combinations

One important interface in any PSA Program occurs between the person constructing the event trees and fault trees and the person evaluating the consequences of the accident. In the case of this program, that interface occurs during the production of the event combination tables. These tables examine each "success" branch point in the event trees and document the assumptions made in determining that the systems were indeed successful in minimizing the extent of release. For example, if the event tree analyst has assumed that one ECC pump running for six months is sufficient following a loss of coolant accident, then the consequence analyst must verify that one pump will cool the fuel and the pump is no longer required after six months.

At this stage, the containment failure possibilities are examined and the relevant failure modes included for downstream analysis. Event categorization in the five regulatory categories is proposed for AECB review at this time also.

e. Safety Analysis Basis Documents (SABs)

Required analysis cases are defined by the consequence analyst based on the assumptions made in the event tree work. All the analysis cases together with the analysis methods, assumptions and proposed acceptance criteria are presented in SABs. While doing this, the analyst also refers back to the

original list of failure modes to ensure that the analysis addresses all of the issues arising from the original list. The SABs are reviewed by AECB prior to start of the analysis.

f. Consequence Analysis

Having defined the analysis to be done and the way it is to be done, the analyst runs the cases and documents the results in a safety report for regulatory review. With respect to the allowable public releases, the analyst uses the limits proposed in Table 1.

g. Safety Analysis Data List (SADL)

The analyst also documents the data being used in the Safety Analysis Data List (SADL). This list is checked by the system designers to ensure the accuracy of the data. One key part of the SADL is the Minimum Allowable Performance Standards (MAPS) for safety systems. This part is eventually passed on to the plant operations group so that they know the safe operating limits for the plant. Sometimes iteration by the consequence analyst is required to determine how safety can best be demonstrated while still allowing operating margins.

h. External Events

At an early stage in the design process, it is difficult to do a rigorous assessment of external events. For example, if the site is not known, then the seismic and meteorological limits for the design have to be chosen based on a typical site or hypothetical limiting site. For the CANDU 3 standard product design, the site conditions are based on values that envelope most sites in potential markets. Another difficulty is that protection for seismic, fire and other external and common cause events depends on good execution in the detailed design. The execution of the concepts is checked by various auditing techniques once the plant design is complete. This is followed up by audits of the completed plant prior to full power operation.

The CANDU 3 has established overall siting requirements in a Plant Performance Specification document. The external events included(see Figure 1) are then examined to determine a design approach based on protection and separation of vital process and mitigating equipment. The design approach is documented in Safety Design Guides (SDG). Compliance with these guides is mandatory unless the exception can pass review by other designers and the regulatory. Compliance with these SDGs is examined by Design Review and regulatory review. Once the design program has been completed, analysis will have been done to establish the adequacy of the protection of systems and the response of mitigation systems. These analyses are documented in Assessment Reports and forwarded for regulatory review.

3. CONCLUSIONS

A systematic plant review of the CANDU 3 design has been completed. This process identified 84 abnormal initiating events for the purpose of PSA and consequence analysis. The review was based on a process which is methodical and auditable. Such a review provides confidence that licensing and risk assessment of the design are well founded.

The overall accident assessment program for the CANDU 3 has been established. Accident analysis for each of the above 84 initiating events will be carried out to demonstrate that the public is adequately protected from the consequences of these events.

The first step in the accident analysis process is to develop event trees which probabilistically examine the effectiveness of the back-up heat sinks and support services for mitigating the accident. This part of the work is now largely complete. Consequence analysis will be carried out to verify event tree assumptions, and to calculate releases to the public. The safety analysis basis documents (SABs) are being prepared which discuss the requirements and methodology of consequence analysis.

4. REFERENCES

(1) ATOMIC ENERGY CONTROL BOARD CONSULTATIVE DOCUMENT C-6, "Proposed Regulatory Guide, Requirements for the Safety Analysis of CANDU Nuclear Power Plants", issued for comment in 1980 June (under revision).

Table 1
Maximum Permissible Reference Doses to the Most Exposed Member of the Public at or Beyond the Site Boundary

Initiating Event Frequency (f)	From AECB Consultative Document C-6		
	Event Class	Reference Individual Dose Limit	
		Whole Body	Thyroid
$f > 10^{-2}$/yr	1	0.0005 Sv (50 mrem)	0.005 Sv (500 mrem)
10^{-2}/yr $\geq f > 10^{-3}$/yr	2	0.005 Sv (500 mrem)	0.05 Sv (5 rem)
10^{-3}/yr $\geq f > 10^{-4}$/yr	3	0.03 Sv (3 rem)	0.3 Sv (30 rem)
10^{-4}/yr $\geq f > 10^{-5}$/yr	4	0.1 Sv (10 rem)	1.0 Sv (100 rem)
$f \leq 10^{-5}$/yr	5	0.25 Sv (25 rem)	2.5 Sv (250 rem)

Note: This frequency/dose criteria will be applied only to those accident sequences which do not result in a severe core damage.

Table 2
Listing of Initiating Events for CANDU 3 PSA/Consequence Analysis

#	Initiating Event Description	#	Initiating Event Description
1	Partial loss of moderator heat sink	2	Partial loss of Class III power
3	Loss of individual DCS stations	4	Loss of communication between DCS & PDS or failure of PDS
5	Loss of one DCS channel	6	Loss of individual I/O modules
7	Loss of group control station as a whole - loss of Channel B	8	Total loss of moderator heat sink
9	Loss of service water	10	Moderator or interfacing system pipe breaks - outside shield tank - tritium release into the R/B

Table 2
Listing of Initiating Events for CANDU 3 PSA/Consequence Analysis

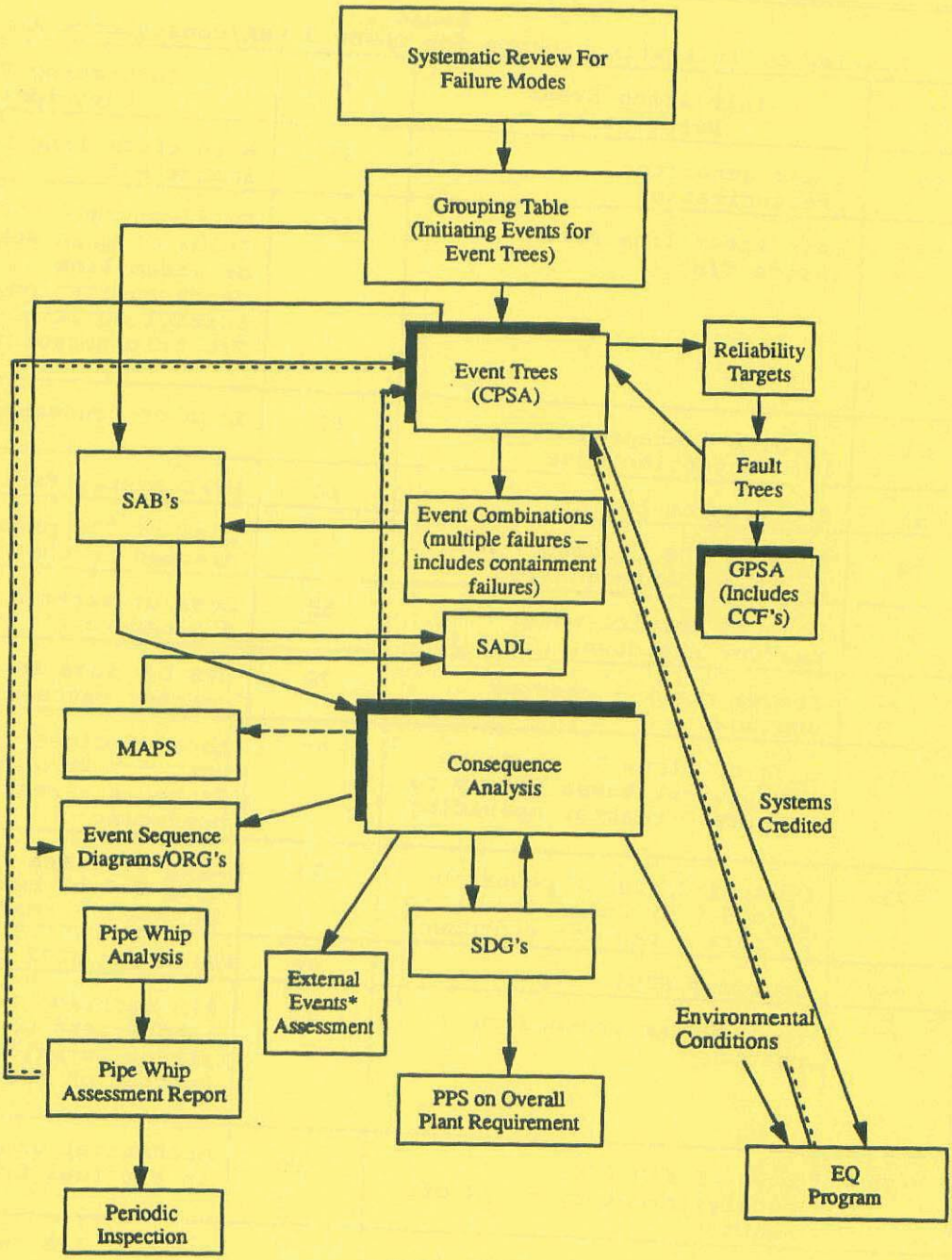
#	Initiating Event Description	#	Initiating Event Description
11	Moderator HX plate(s) failure - tritium release into GP1 RCW	12	Inadvertent discharge of moderator D_2O to the interfacing system(s) outside the R/B - potential for tritium discharge outside the R/B
13	Moderator pipe break inside the shield tank/calandria vessel failure/ spurious demin H_2O make-up to calandria	14	Calandria drain line break outside the shield tank, upstream of V16
15	Spurious actuation of moderator relief devices	16	Loss of instrument air
17	Partial loss of Class II power	18	Calandria tube failure
19	Moderator deuterium excursion	20	LISS pipe break downstream of the poison injection tanks and outside/inside the shield tank
21	Partial loss of Class I power	22	Loss of shield cooling system heat sink
23	Loss of shield cooling system inventory Case i - pipe breaks Case ii - lattice tube failure Case iii - end shield leaks into F/M vault	24	End fitting break
25	End fitting break inside the annulus gas system - CTX fails	26	Feeder break
27	Pressure tube and calandria tube rupture	28	Feeder stagnation break
29	All HTS pump seals fail - D_2O unavailable	30	Miscellaneous small LOCA events - discharge into R/B
31	F/M backing off without channel shield plug, latched spacer plug and channel closure being replaced - fuel ejection into F/M vault	32	Large LOCA

Table 2
Listing of Initiating Events for CANDU 3 PSA/Consequence Analysis

#	Initiating Event Description	#	Initiating Event Description
33	Very small LOCA events - discharge into containment and within D_2O feed capability	34	D_2O storage tank failure
35	Loss of F/M D_2O inventory due to hose failure (F/M in reactor)	36	Steam generator tube rupture (single tube)
37	Steam generator multiple tube rupture (10 tubes)	38	HTS D_2O loss into GP1 RCW system
39	Blowback from HTS into ECC (inadvertent opening of a HTS/ECC header isolation and H_2O isolation valves and gross internal leakage from the ECC check valve)	40	LRV spuriously fails open
41	Pressurizer relief valve spuriously fails open	42	HTS pressure control failure - low
43	HTS pressure control failure - high	44	Partial loss of HTS flow due to failure of one pump i. HT pump trip ii. HT pump failure due to bearing seizure/impeller failure/drive shaft failure
45	Spurious closure of pressurizer isolation valve (63331-MV43)	46	Bleed condenser spray spuriously turned on or excessive spray flow
47	Bulk core power excursion i. reactor operating ii. reactor shut down (LOR during shutdown)	48	Regional core power excursion
49	Reactor stepback	50	Total loss of GP1 feedwater flow
51	Feedwater pipe breaks in the T/B	52	Feedwater pipe breaks in the R/B, upstream of the steam generator check valve
53	Feedwater pipe breaks downstream of the steam generator check valve in the R/B	54	Boiler blowdown line break between the steam generator and blowdown isolation valve
55	Boiler blowdown line break - rupture between the blowdown isolation valve and the R/B wall	56	Boiler blowdown line break - rupture between the R/B wall and the flash tank

Table 2
Listing of Initiating Events for CANDU 3 PSA/Consequence Analysis

#	Initiating Event Description	#	Initiating Event Description
57	Steam generator pressurization	58	Main steam line break inside R/B
59	Main steam line break inside T/B	60	Small steam line break (<10% of main steam line) or steam line depressurization leading to initial SG level surge to T/G trip setpoint
61	Turbine overspeed during load rejection mode	62	Loss of condenser vacuum
63	BPC program failure	64	HVAC system failure
65	Loss of SDC process - HTS full and depressurized	66	Loss of SDC process - HTS drained to the header level
67	Loss of service water - reactor shutdown, HTS full	68	Loss of service water - HTS drained to the header level
69	Feeder break - reactor shutdown	70	HTS D_2O loss into GP1 RCW - reactor shutdown
71	Loss of Class IV power to both 6.9 kV buses for up to 2 hours - reactor operating	72	Loss of Class IV power to both 6.9 kV buses from 2 to 24 hours - reactor operating
73	Loss of Class IV power to both 6.9 kV buses for up to 2 hours - reactor shutdown	74	Loss of Class IV power to both 6.9 kV buses from 2 to 24 hours - reactor shutdown
75	Spurious SDS1 trip	76	Spurious SDS2 trip
77	Fuel bundle crushed on reactor	78	F/M carriage tilt or inadvertent movement in X/Y direction while F/M is latched on reactor
79	Loss of F/M D_2O supply/inventory - F/M off reactor	80	Mechanical damage to fuel in the fuel transfer port
81	Fuel transfer failures from the transfer port to the IFB	82	Loss of IFB heat sink
83	Loss of IFB inventory Case i. pipe failures Case ii. liner failures Case iii. minor damage to IFB walls/floor	84	Failure of the IFB ventilation system



Legend: CPSA – Conceptual Probabilistic Safety Analysis
GPSA – Generic Probabilistic Safety Analysis
SAB's – Safety Analysis Basis Documents
EQ – Environmental Qualification
ORG's – Operator Responsible Guidelines
PPS – Plant Performance Specification
CCF's – Common Cause Factors
SDG's – Safety Design Guides
MAPS – Minimum Allowable Performance Specification
SADL – Safety Analysis Data List

* Includes: – Tornadoes – Earthquakes – Missiles
– Fires – Floods (internal and external) – Objects falling on R/M deck

Figure 1 – CANDU 3 Accident Assessment Program