



CANDU Safety

#20 - Probabilistic Safety Analysis

V.G. Snell
Safety & Licensing

R. Jaitly
CANDU 6/9 PSA



Topics

- λ **What is a PSA?**
- λ **History**
- λ **Acceptance Criteria**
- λ **Elements Of PSA**
- λ **PSA as a Decision Making Tool**
- λ **Results of CANDU PSAs**
- λ **Recent PSA Developments**



Use of Probabilistic Safety Analysis (PSA)

- λ provides a numerical measure of plant risk to the public
 - identifies the potential accidents, calculates their probability of occurrence, and their consequences
 - the product of frequency of postulated accidents and their consequences provides an estimate of plant risk
- λ develops mathematical model that relates plant risk to contributory factors: plant configuration, equipment reliability, operator error probability, operating practices, plant response, and system capability
- λ design assist & audit tool
 - fix it first, not calculate it after



PSAs by AECL

- λ first probabilistic assessment: Douglas Point (1960s)
- λ early PSAs for CANDU 6, Pickering B, Bruce B (1978 to 1983)
- λ CANDU 6 PSA with KEMA (The Netherlands) (1985-1987)
- λ Wolsong 2, 3 & 4 PSA (1992-1996)
- λ CANDU 9 PSA (1995-)
- λ Qinshan 1 & 2 PSA (1997-)



PSAs by Others

λ Ontario Hydro

- Darlington Risk Assessment (1987-88)
- Pickering "A" Risk Assessment (1995)
- Bruce "B" Risk Assessment (in progress)

λ Korea

- Wolsong 2 PSA with external events (1998)

λ Romania

- PSA studies on Cernavoda 1 (in progress)



PSA Acceptance Criteria

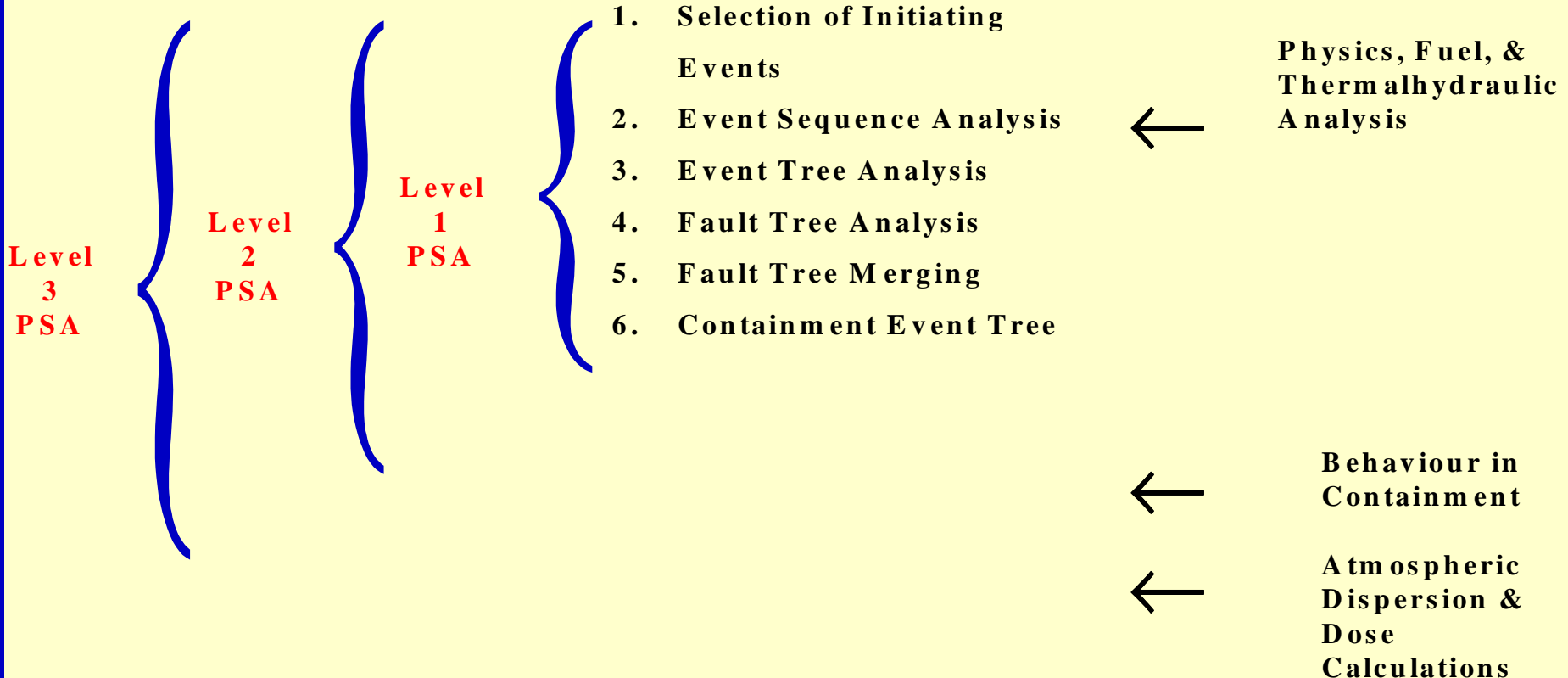
- λ Level 1 PSA acceptance criteria: guide to designers, *not* a regulatory target**
 - frequency of individual event sequences resulting in severe core damage $< 10^{-6}$ events per year**
 - frequency of individual event sequences requiring moderator to function as heat sink $< 10^{-5}$ events per year**
- λ related to Safety Goals in earlier lecture**



PSA Scope

Steps in PSA Analysis

Consequence Analysis Input to Process





Elements of PSA

- λ Identification of Initiating Events
- λ Event Sequence Diagrams
- λ Event Tree Analysis
- λ Fault Tree Analysis
- λ Human Reliability Analysis
- λ Accident Sequence Quantification
- λ Recovery Analysis
- λ Common Cause Failure Analysis
- λ Uncertainty & Sensitivity Analysis
- λ Level 2 & Level 3 PSA

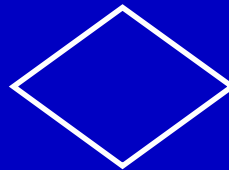


Worked Example - A Car Braking System

- λ Event tree: What are the consequences of failure of the normal car braking system?
- λ Fault tree: What is the probability of failure of the normal car braking system on demand?



Basic Event



Undeveloped Event



Intermediate Event



A Few Symbols

λ AND gate:

- event A AND event B must occur in order for event C to occur



λ OR gate:

- event A OR event B must occur in order for event C to occur





Event Tree - Example

Car brakes fail
on demand

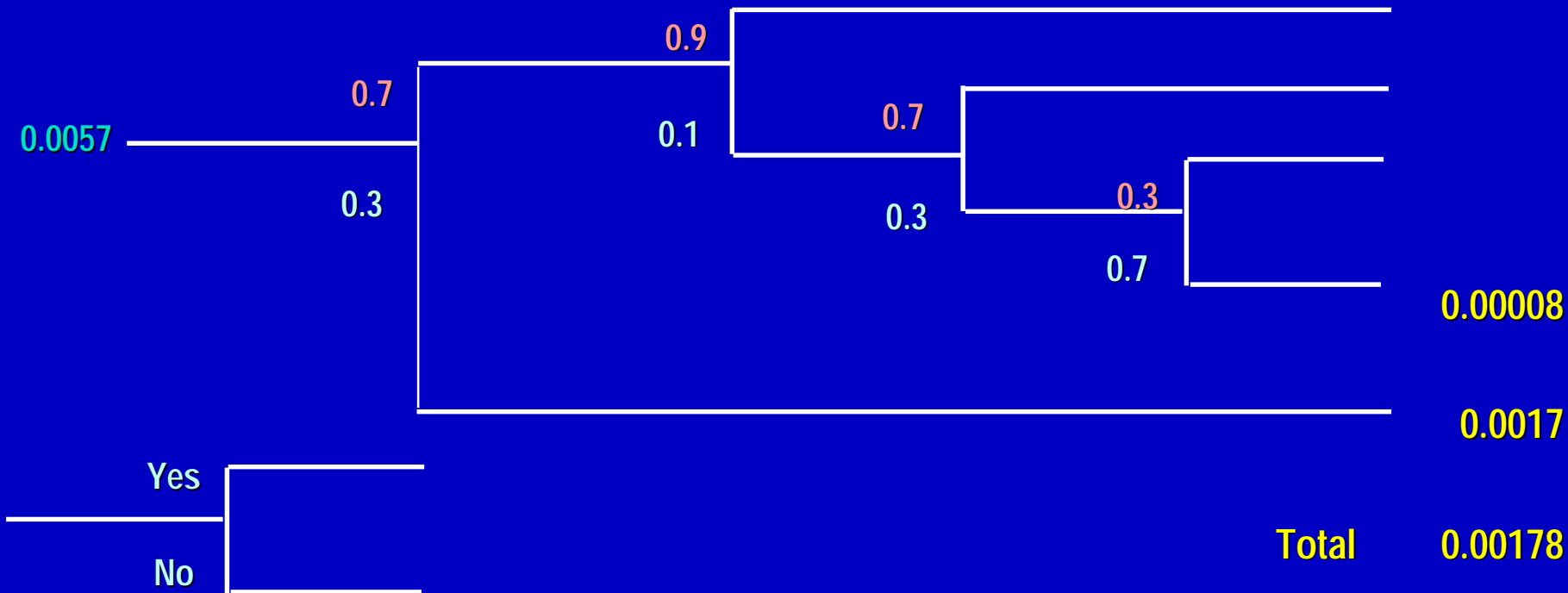
Operator

Emergency
Brakes

Down-
shift

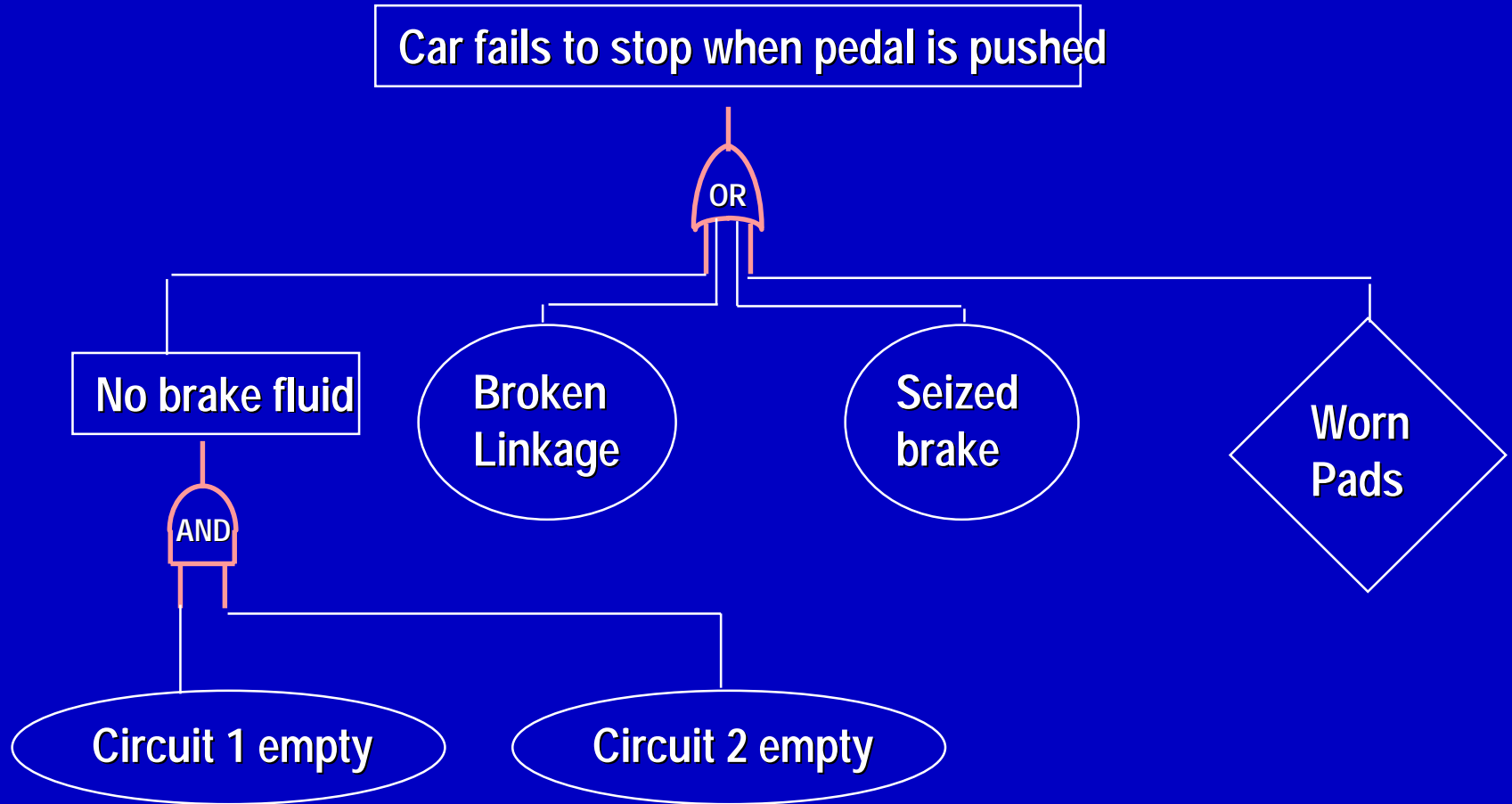
Engine

Crash
Probability



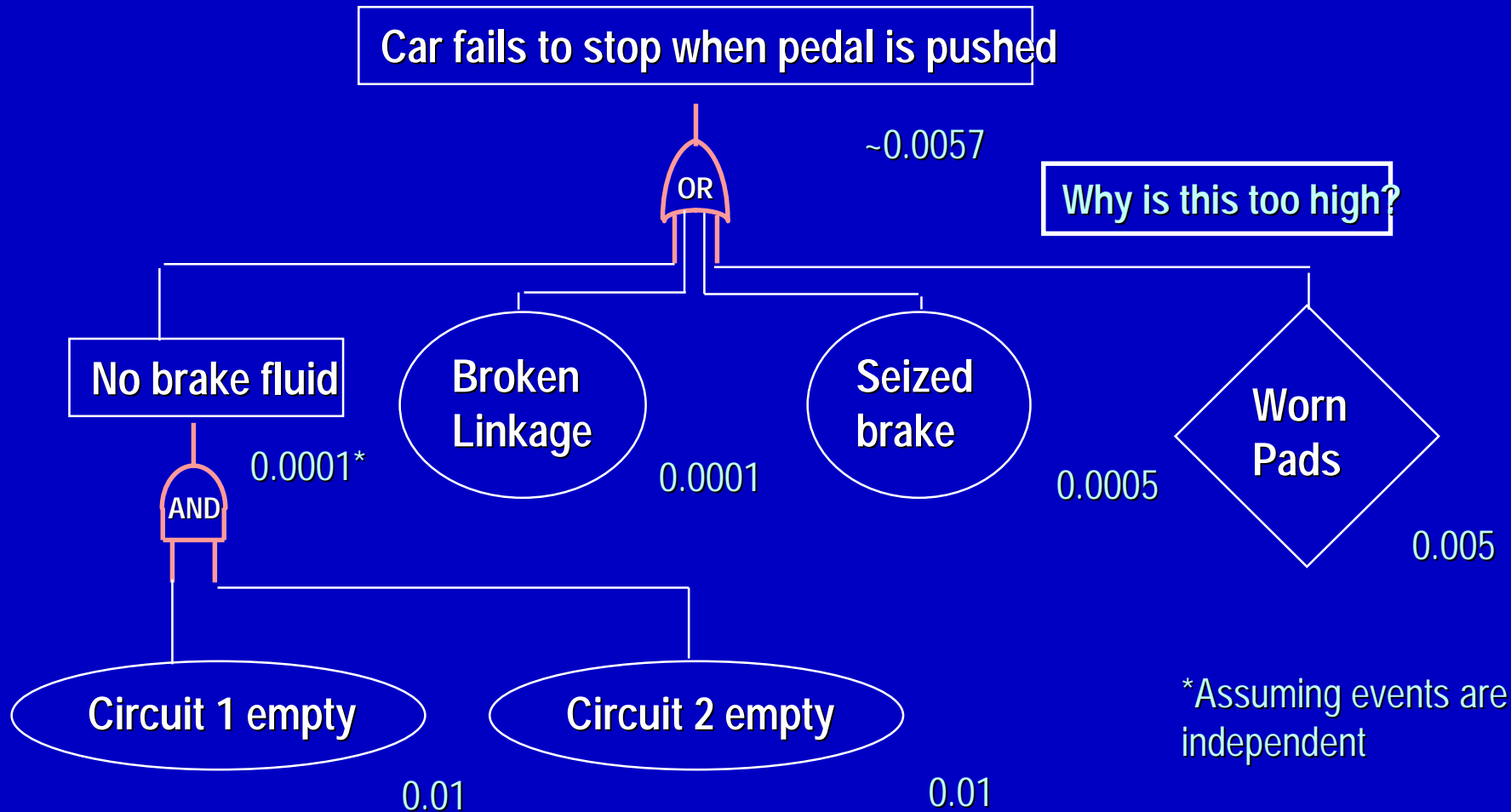


Fault tree - Example





Fault Tree with Sample Demand Probabilities





Event Tree - Nuclear Power Plant

- λ an event tree represents various possible scenarios which can result from the same initiating event
- λ the end-point of an event tree is either a stable condition or a Plant Damage State
- λ quantitatively it ties together the reliability of different systems
- λ fault tree analysis and operating experience is used to estimate initiating event frequency



Typical Event Tree Branch Points for CANDU

1. Initiating Event
2. Reactor Shutdown
3. Bleed Condenser Bottle-up if LRVs opened
4. Class IV Power Available
5. Group 1 Odd Class III Energized
6. Group 2 Odd Class III Energized
7. Group 1 Even Class III Energized
8. Group 2 Even Class III Energized
9. Instrument Air Available
10. Service Water Available
11. Operator Action
12. Preferred Heat Sink
13. Alternate Heat Sink



Typical Fault Trees for CANDU

- λ loss of electrical power
- λ loss of feedwater
- λ steam main break
- λ loss of coolant accident
- λ loss of flow
- λ loss of computer control
- λ loss of support services:
 - instrument air, process water
- λ loss of reactivity control
- λ etc.



Fault Tree Analysis

- λ identifies:
 - most likely system failure modes
 - potential weaknesses in system design and operation
- λ basic events include random equipment failures, human errors, and test and maintenance unavailabilities
- λ component failure database from various sources:
 - Darlington Risk Assessment
 - IEEE Standard 500
 - Nuclear Plant Reliability Data System
 - IAEA Tech Doc 478
 - Point Lepreau observed component reliability report



Level 2 PSA

- λ Level 1 PSA *plus* containment performance & source terms at containment boundary
- λ requires severe core damage accident analysis for beyond-design-basis events identified in the Level 1 PSA, e.g.:
 - core debris formation & progression
 - thermohydraulics of core debris in calandria
 - hydrogen production
 - containment performance



PSA Role in Severe Accident Mitigation Design

- λ PSA gives a precise definition of severe accident sequences including the identification of support system failures. This helps assess the adequacy of:
 - long term containment mitigating features (e.g. support services for air coolers, hydrogen control)
 - long term heat removal capability of shield cooling and moderator systems



PSA - Design Assist Role

- λ safety design assistance at an early stage - ensure adequate redundancy & functional separation**
- λ identify risk-dominant accident sequences**
- λ obtain an understanding of the integrated plant response to abnormal events**
- λ identify operator actions & provide input to control centre design & Emergency Operating Procedures**
- λ provide input to Environmental Qualification programme**
- λ provide input to test & maintenance programmes**



PSA Has Resulted in Changes During Design

Station Design Change Requests (DCRs) from PSA studies

<u>STATION</u>	<u>APPROVED REQUEST</u>
Gentilly-2	92
Point Lepreau Unit 1	66
Wolsong Unit 1	37
Pickering "B"	22
Bruce "B"	17

Approximately 80% of the approved design changes were with the balance of plant and service systems (non-nuclear portion).



Design Changes Identified by Darlington PSA

λ	number of design problems identified (and changes made)	105
λ	breakdown of changes:	
	– process control	74%
	– process or equipment arrangement	12%
	– power supply allocation	6%
	– equipment design	4%
	– others	4%



Design Changes Identified by Wolsong 2 PSA

- λ ECC design changes
 - automatic start of recovery pumps
 - greater redundancy for certain valves
 - increased test frequency of certain valves
- λ improved design for heat transport system pump high bearing temperature automatic trip
- λ for screen wash system, change failure position of certain valves to “fail close” on loss of instrument air
- λ code classification upgrade for boiler blowdown piping inside containment



CANDU 9 Enhancements Based on Earlier PSAs

- λ improved feedwater reliability**
 - 2 independent sources of high pressure feedwater
 - auxiliary diesel-driven pump
- λ two groups of service water supply to shutdown cooler**
- λ 4 onsite diesel-generators - low station blackout frequency**
- λ improved ECC reliability**
 - elimination of check valves
 - automatic recirculation phase
 - sustained low Reactor Outlet Header pressure conditioning
 - elimination of medium pressure ECC



CANDU 9 Changes Supported by PSA

- λ automatic heat transport system pump trip on high bearing temperature
- λ passive make-up capability to heat transport system, moderator, boilers & end-shields
- λ moderator make-up from reactor building floor
- λ relocation of service water pumps for protection against steam line break



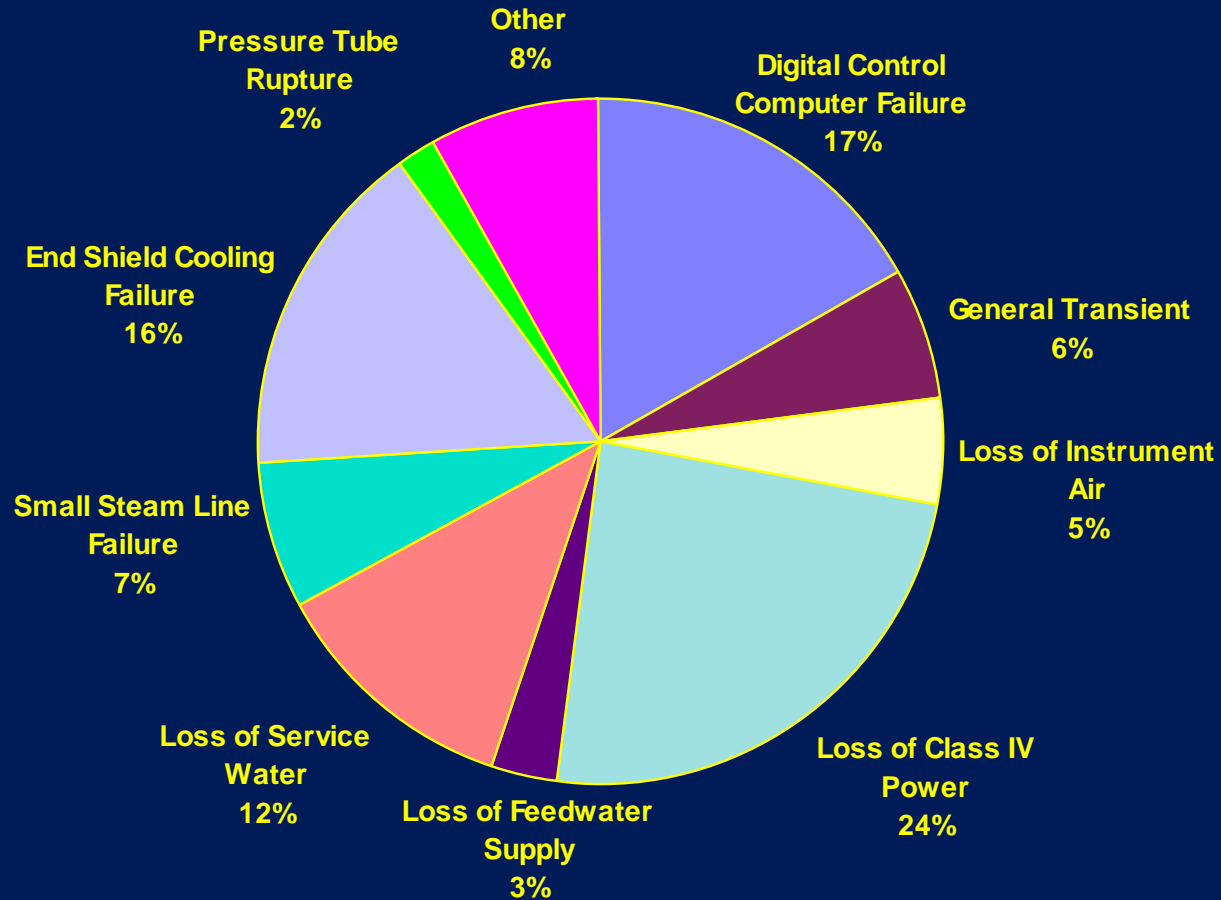
Summary of CANDU PSA Results (Internal Events)

- λ Summed severe core damage frequency for Wolsong 2
= $6.1 \times 10^{-6}/\text{yr}$.
- λ Summed severe core damage frequency for Darlington
= $3.8 \times 10^{-6}/\text{yr}$.
- λ Summed severe core damage frequency for CANDU 6 (KEMA)
= $4.6 \times 10^{-6}/\text{yr}$.
- λ Summed severe core damage frequency due to failure to
shutdown
= $3 \times 10^{-8} / \text{yr}$. (typical)



Wolsong 2 Summed Severe Core Damage Frequency

Summation = 6.1 E-6 Events/Year





Recent CANDU PSA Related Developments

- λ detailed PSA for “beyond-design-basis” external events (seismic, fire, flooding)**
 - Korean study is instructive**
 - AECL programme underway to review CANDU 6 & CANDU 9**
- λ Common Cause Failure Analysis**
- λ tests & models for CANDU severe accident progression**
- λ increased use of PSA models / insights in the day-to-day running of stations:**
 - outage planning**
 - risk impact of changes in plant configuration, test frequencies, on line equipment maintenance**



Conclusions

- λ PSA is most cost-effective when used as a design tool because the plant can be strengthened before it is built**
- λ core damage frequencies for CANDU reflect the role of the moderator (but do not credit the time delay due to shield tank)**
- λ PSA can be used in outage planning, configuration changes & maintenance on operating stations**
- λ beyond-design-basis external events have been analyzed by Korea and are part of AECL's current review of CANDU 6 / 9**