CANDU Safety
#20 - Probabilistic Safety Analysis

V.G. Snell
Safety & Licensing

R. Jaitly
CANDU 6/9 PSA

Topics

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

Use of Probabilistic Safety Analysis (PSA)

- **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**
- **develops mathematical model that relates plant risk to contributory factors: plant configuration, equipment reliability, operator error probability, operating practices, plant response, and system capability**
- **design assist & audit tool**
  - **fix it first, not calculate it after**

PSAs by AECL

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

PSAs by Others

- Ontario Hydro
  - Darlington Risk Assessment (1987-88)
  - Pickering “A” Risk Assessment (1995)
  - Bruce “B” Risk Assessment (in progress)
- Korea
  - Wolsong 2 PSA with external events (1998)
- Romania
  - PSA studies on Cernavoda 1 (in progress)

PSA Acceptance Criteria

- **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**
- **related to Safety Goals in earlier lecture**

PSA Scope

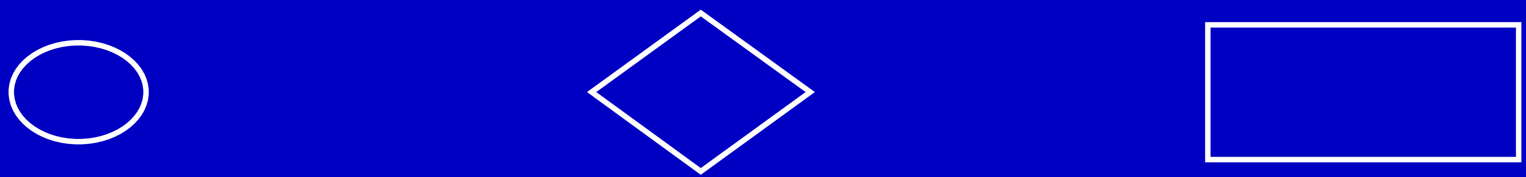
			Steps in PSA Analysis	Consequence Analysis Input to Process
Level 3 PSA	Level 2 PSA	Level 1 PSA	1. Selection of Initiating Events	
			2. Event Sequence Analysis	← Physics, Fuel, & Thermalhydraulic Analysis
			3. Event Tree Analysis	
			4. Fault Tree Analysis	
			5. Fault Tree Merging	
			6. Containment Event Tree	
				← Behaviour in Containment
				← Atmospheric Dispersion & Dose Calculations

Elements of PSA

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

Worked Example - A Car Braking System

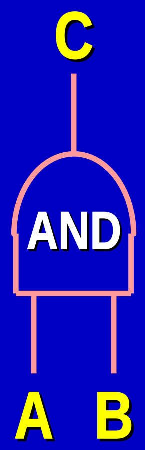
- Event tree: What are the consequences of failure of the normal car braking system?
- Fault tree: What is the probability of failure of the normal car braking system on demand?



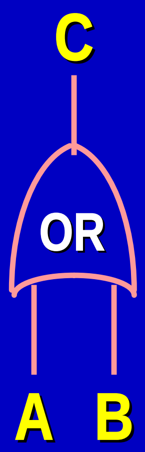
Basic Event | **Undeveloped Event** | **Intermediate Event**

A Few Symbols

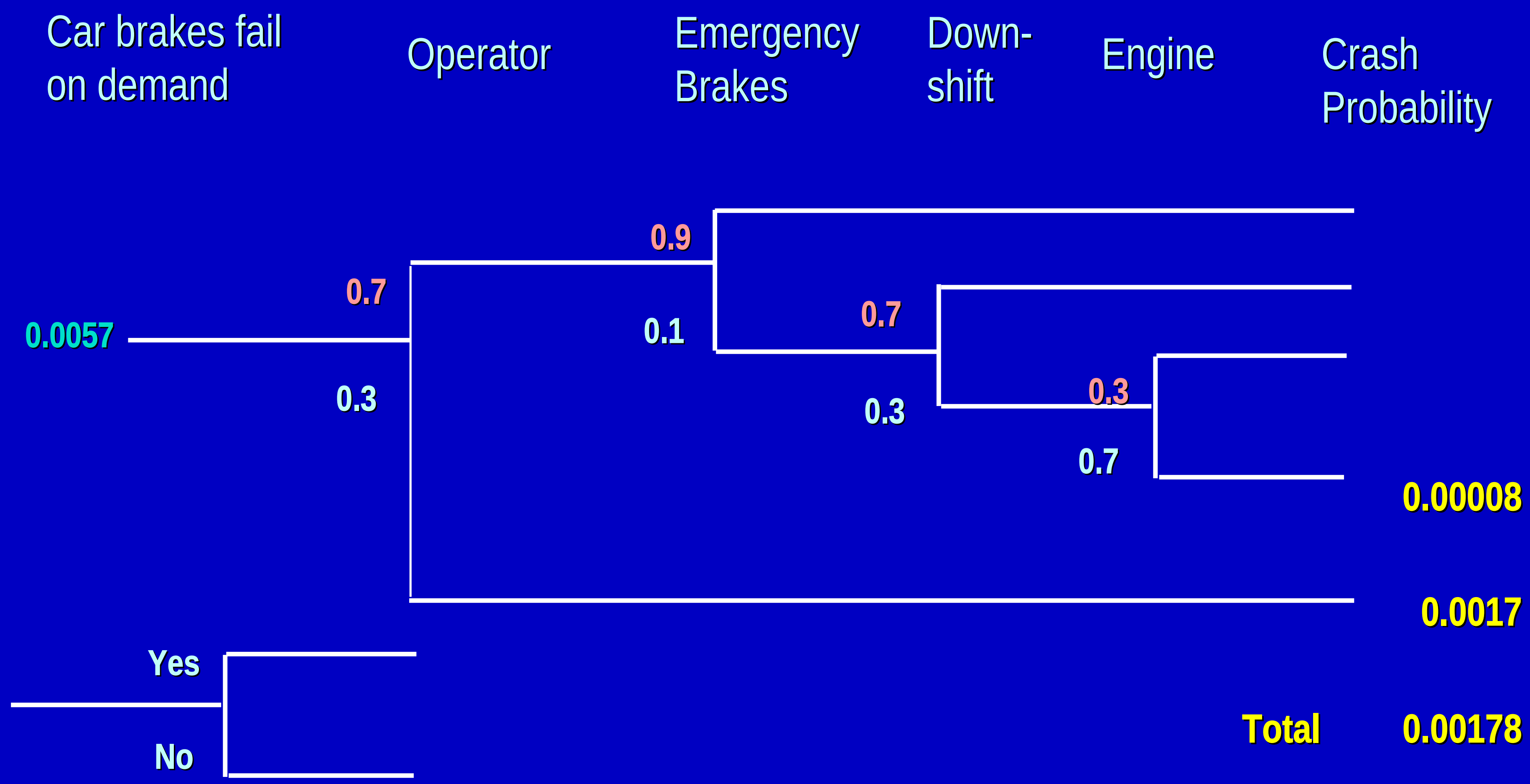
- AND gate:
  - event A AND event B must occur in order for event C to occur



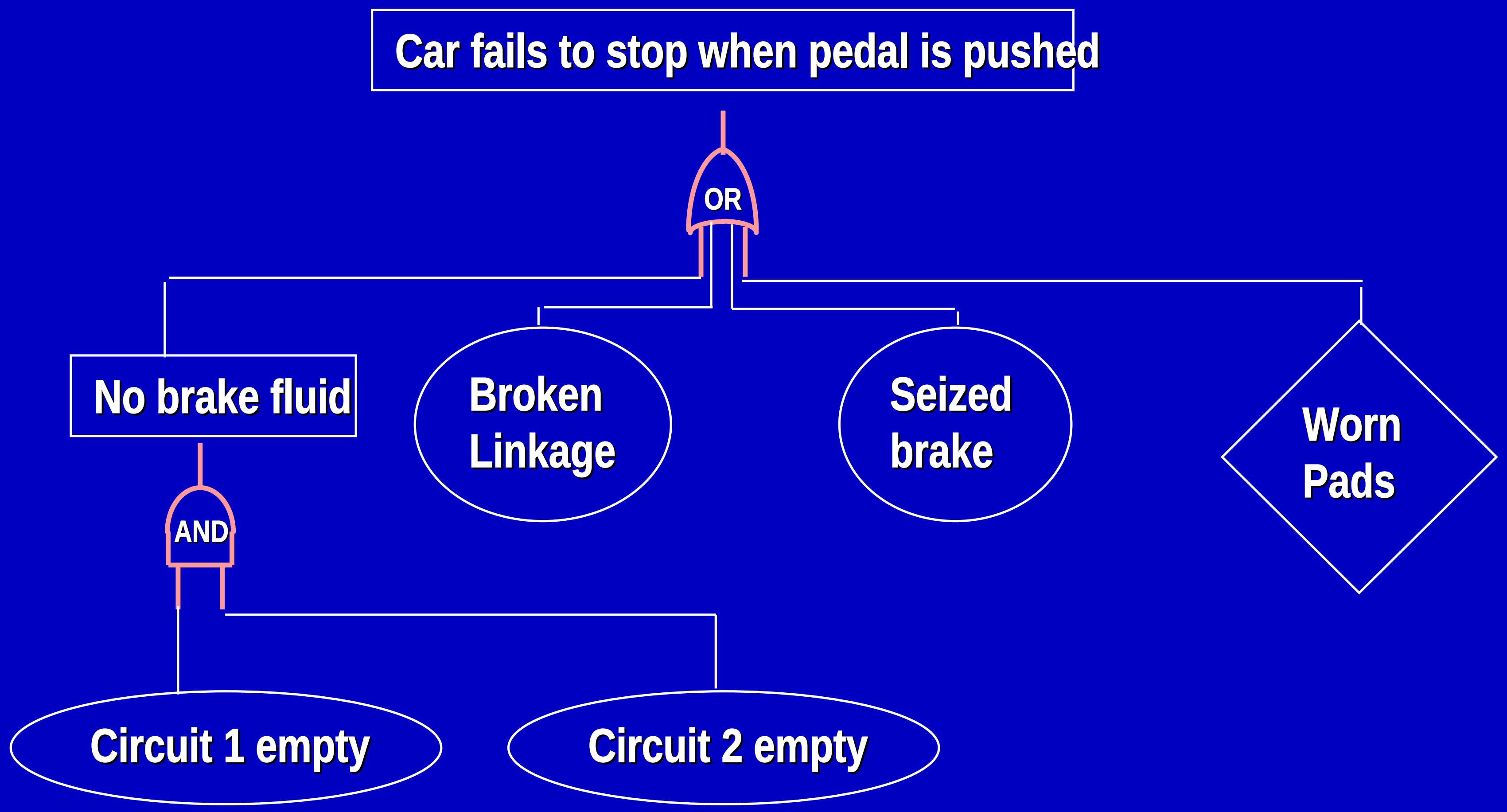
- OR gate:
  - event A OR event B must occur in order for event C to occur



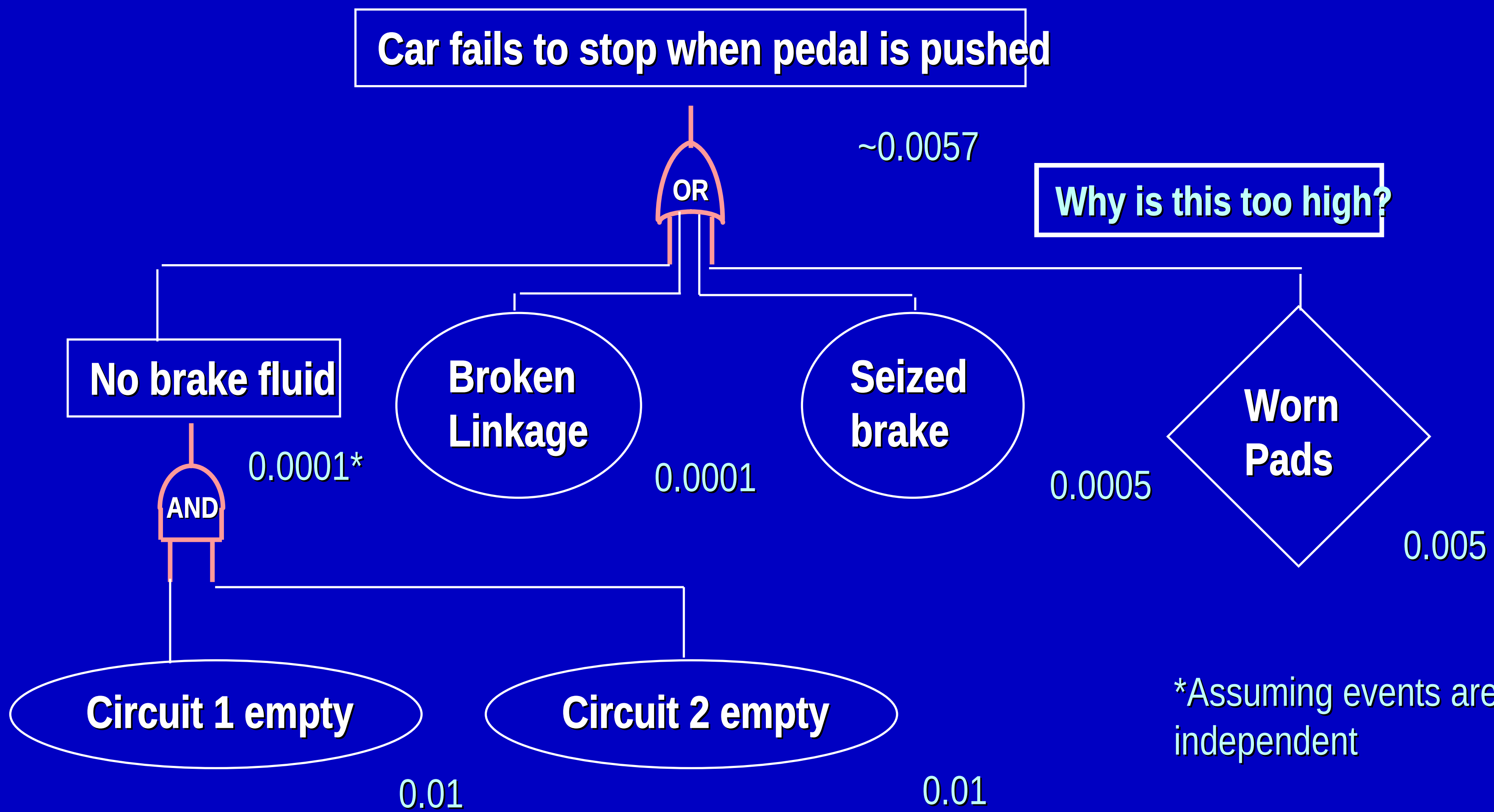
Event Tree - Example



Fault tree - Example



Fault Tree with Sample Demand Probabilities



*Assuming events are independent

Event Tree - Nuclear Power Plant

- **an event tree represents various possible scenarios which can result from the same initiating event**
- **the end-point of an event tree is either a stable condition or a Plant Damage State**
- **quantitatively it ties together the reliability of different systems**
- **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

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

Fault Tree Analysis

- identifies:
  - most likely system failure modes
  - potential weaknesses in system design and operation
- basic events include random equipment failures, human errors, and test and maintenance unavailabilities
- 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

- **Level 1 PSA *plus* containment performance & source terms at containment boundary**
- **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

- 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

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

PSA Has Resulted in Changes During Design

Station Design Change Requests (DCRs) from PSA studies

STATION	APPROVED REQUEST
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

number of design problems identified (and changes made)	105
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

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

CANDU 9 Enhancements Based on Earlier PSAs

- improved feedwater reliability
  - 2 independent sources of high pressure feedwater
  - auxiliary diesel-driven pump
- two groups of service water supply to shutdown cooler
- 4 onsite diesel-generators - low station blackout frequency
- 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

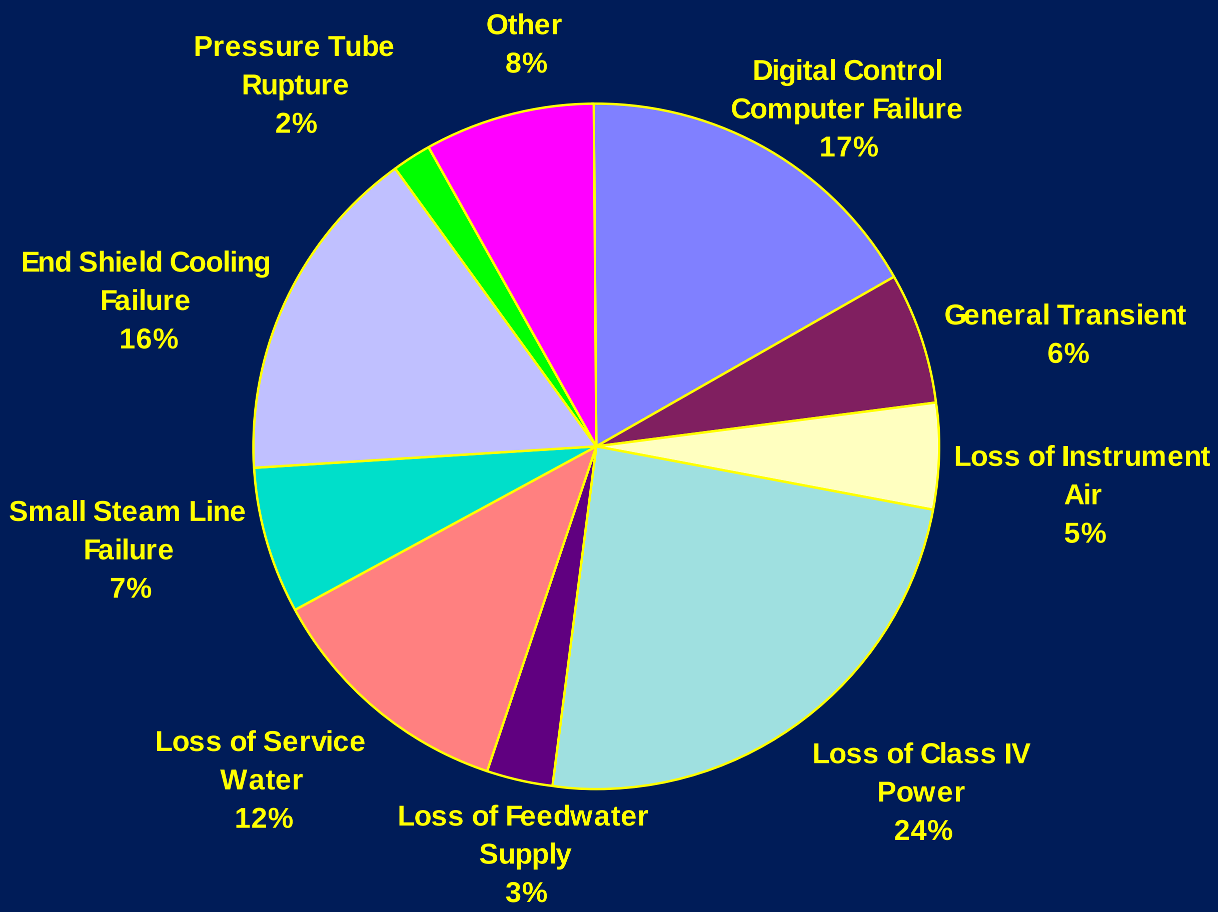
- **automatic heat transport system pump trip on high bearing temperature**
- **passive make-up capability to heat transport system, moderator, boilers & end-shields**
- **moderator make-up from reactor building floor**
- **relocation of service water pumps for protection against steam line break**

Summary of CANDU PSA Results (Internal Events)

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

Wolsong 2 Summed Severe Core Damage Frequency

Summation = 6.1 E-6 Events/Year



Recent CANDU PSA Related Developments

- detailed PSA for “beyond-design-basis” external events (seismic, fire, flooding)
  - Korean study is instructive
  - AECL programme underway to review CANDU 6 & CANDU 9
- Common Cause Failure Analysis
- tests & models for CANDU severe accident progression
- 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

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