Risk

Dr. V.G. Snell
Director
Safety & Licensing

Contents

- What is Risk?
- Some Everyday Examples
- Safety Goals for Nuclear Power Plants
- How Is Risk Calculated?
- Worked Example - A Car Braking System
  - Cross Links
- Sample Results for Nuclear Power Plants
- Conclusions

What Is Risk?

Risk = Frequency of an event x consequences of the event

- **Examples of risk:**
  - **annual individual risk of death**
  - **annual nuclear plant risk of core damage**
  - **annual nuclear plant risk of a large release of radioactivity**
  - **risk of psychotic reaction to malaria drug, per dose**

Safest and Most Dangerous Occupations*

Occupation	Fatalities / 100,000 / year
Administrative support, clerical	1
Executive & Managerial	3
News Vendors	16
Police	17
Truck drivers	26
Farm Workers	30
Construction labourers	39
Miners	78
Pilots & navigators	97
Lumberjacks	101
Sailors	115

*US, 1995

“Acceptable” (since accepted) Occupational Risk?

5 per 100,000 per year (5 x 10^{-5} per year)

to

100 per 100,000 per year (1 x 10^{-3} per year)

Non-Occupational Accidental Fatalities*

Accident	Fatalities / 100,000 / year
Lightning	.06
Poisoning	1.5
Firearms	1.1
Drowning	3.6
Fires	3.6
Falls	8.6
Motor vehicle	27

*US, 1970

“Acceptable” (since accepted) Public Risk?

4 per 100,000 per year (4 x 10^{-5} per year)

to

27 per 100,000 per year (3 x 10^{-4} per year)

Total risk of accidental death = 4 x 10^{-4} per year

Note that these are population-average risks

Some groups will be considerably more (or less) at risk than others.

Many Factors Determine "Acceptability"

- **occupational risk vs. public risk**
- **presence of offsetting benefit**
- **voluntary vs. involuntary risk**
  - **can one really eliminate risk from motor vehicles by not driving??**
- **"dread" factor (cancer vs. automobile accident)**
- **perceived ability to control risk**
- **knowledge and familiarity (coal mining vs. operating nuclear plant)**

Safety Goals for Nuclear Power Plants

- Safety goal - an acceptable value of risk
  - risk from NPPs chosen to be very small in comparison to comparable activities
  - e.g., Canada in 1960s - "five times safer than coal"
- Risk of prompt fatality from NPP should be << risk of prompt fatality from all other causes
- Risk of fatal cancer from NPP should be << risk of cancer from all other causes

Risk of fatal cancer *just* from "natural" radiation in Canada =

$$0.002\,\text{Sv/year} \times 0.02\ \text{cancers/Sv} = 4 \times 10^{-5}\ \text{per year}$$

(according to linear dose-effect hypothesis)

Numerical Safety Goals for Nuclear Power Plants

- **For existing nuclear power plants:**
  - **risk of a severe core damage accident must be < 10^{-4} per plant per year**
  - **risk of a large release must be < 10^{-6} per plant per year**
- **For new nuclear power plants:**
  - **factor of 10 lower on both counts**
- **What other industries set safety goals? (think of at least two)**

How is Risk Calculated?

- **For frequent events - easy - just collect the *observed* statistics**
- **For rare events - build up from combinations of more frequent components**
- **e.g., risk / year of a plane crashing on the Skydome =**

  risk of a plane crash per kilometer of steady flight

  × **number of flights / year landing or taking off from Toronto airport**

  × **fraction of flights which fly over Skydome**

  × **diameter of Skydome in km.**

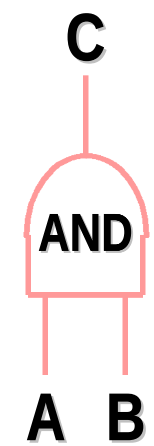
  – **does not account for evasive action, skyjacking**

Fault trees and Event trees

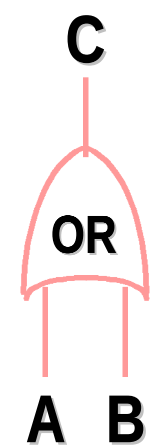
- to determine the risk from rare events:
  - calculate frequency or probability of a system failure (fault tree)
  - calculate consequences of the system failure (event tree)
  - in the event tree, assume each mitigating system either works or fails; if it fails, account for the probability of failure
- end result is the frequency or probability and consequences of a family of events

A Few Symbols

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

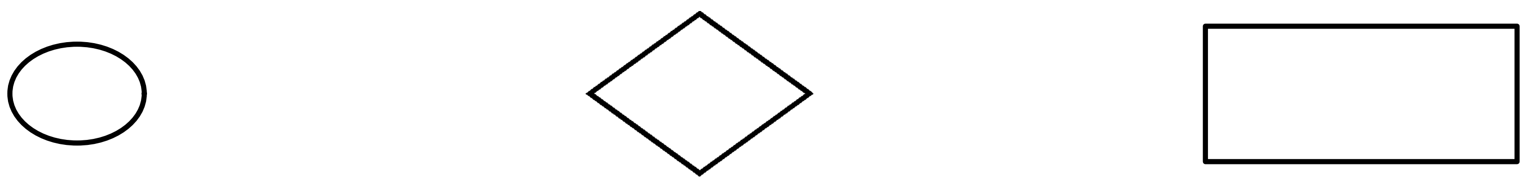


- OR gate:
  - event A OR event B must occur in order for event C to occur



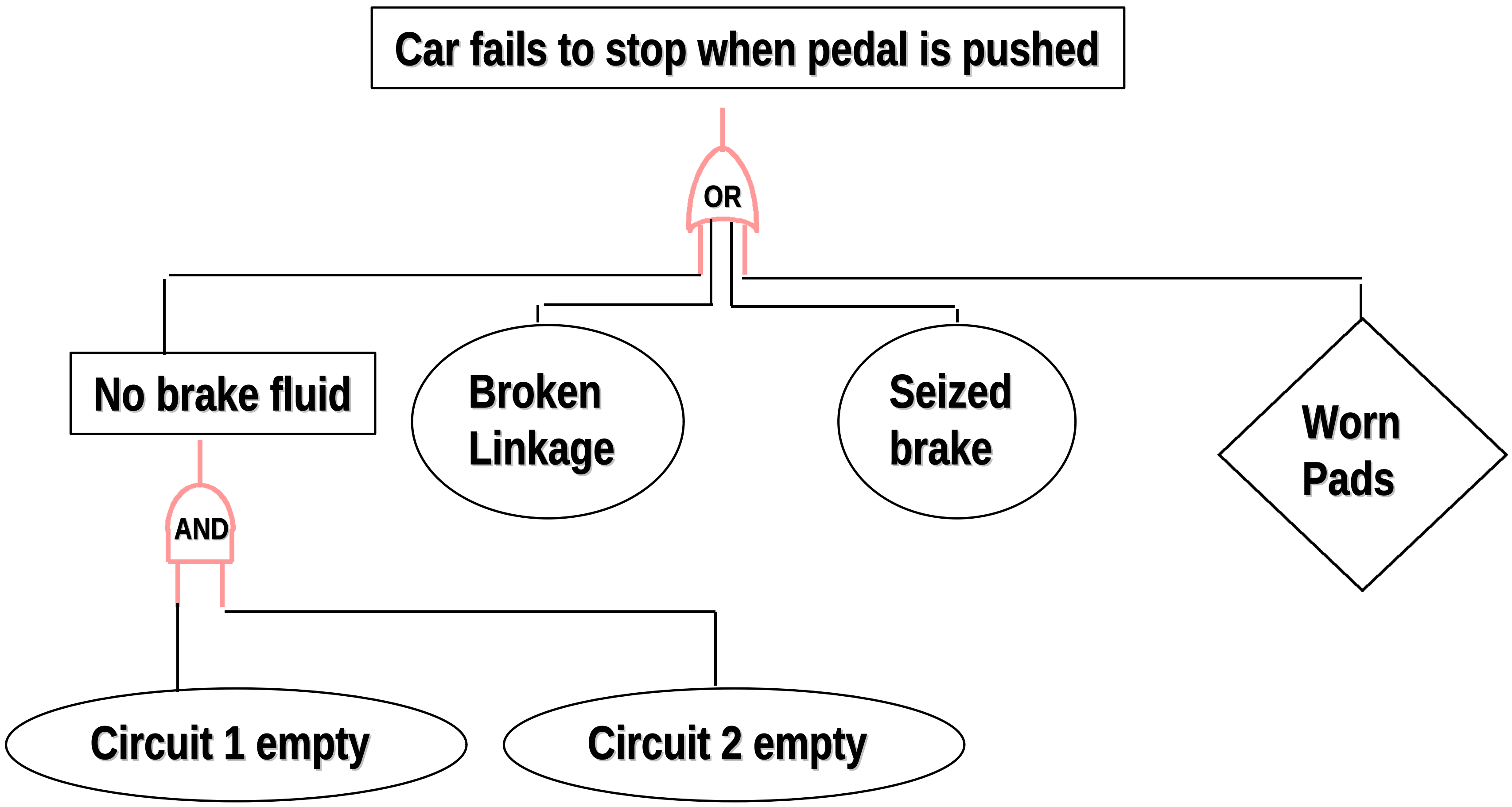
Worked Example - A Car Braking System

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

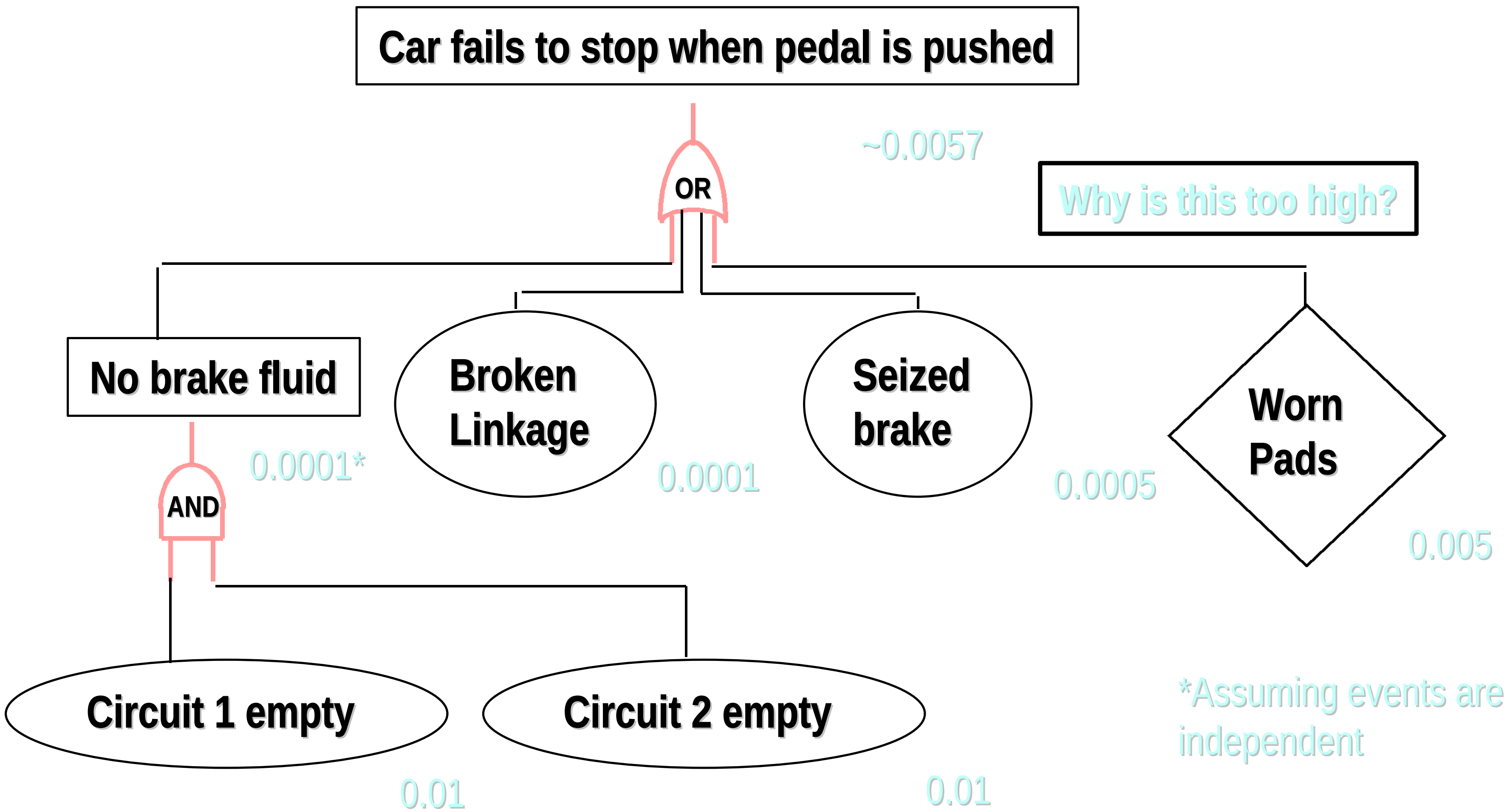


Basic Event **Undeveloped Event** **Intermediate Event**

Fault tree


Car fails to stop when pedal is pushed
OR
No brake fluid
Broken Linkage
Seized brake
Worn Pads
AND
Circuit 1 empty
Circuit 2 empty

Fault Tree with Sample Demand Probabilities



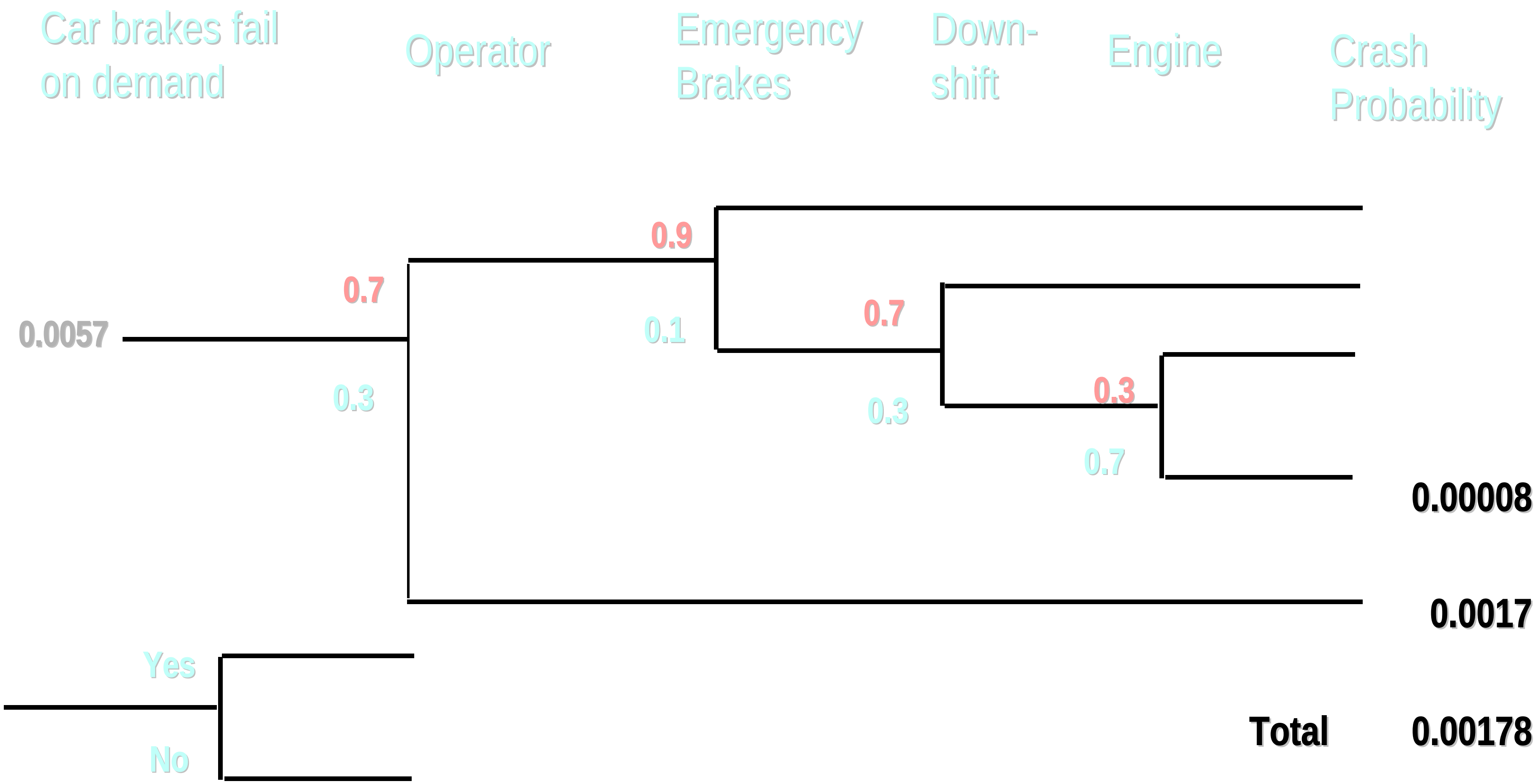
Observations

- using two independent components or subsystems greatly reduces the contribution of a particular failure mode
  - probabilities multiply - except for cross link failures!
- failure probability can be greatly influenced by:
  - preventative maintenance (worn pads)
  - testing (broken linkage)
  - inspection (empty cylinders)
  - quality of materials

What Are the Mitigating Systems?

- **emergency brakes**
- **downshifting**
- **turning off ignition**
- **steering to avoid accident...**
- **need human for all of them**

Event Tree


Car brakes fail on demand
Operator
Emergency Brakes
Down-shift
Engine
Crash Probability
0.0057
0.7
0.3
0.9
0.1
0.7
0.3
0.3
0.7
0.00008
0.0017
Yes
No
Total
0.00178

Cross-Links make probabilities not independent

- **common cause failure**
  - **common maintenance errors**
  - **common fabrication errors**
- **common component failure**
  - **failure of the brake reservoir will drain *both* braking circuits**
  - **both emergency brake and regular brake share same shoes**
- **common support system**
  - **e.g., failure of air conditioning in a control room can cause multiple computer failures**
- **external event - fire, earthquake, tornado**
- **common harsh environment**

Nuclear Power Plants - Fault Trees

- 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.

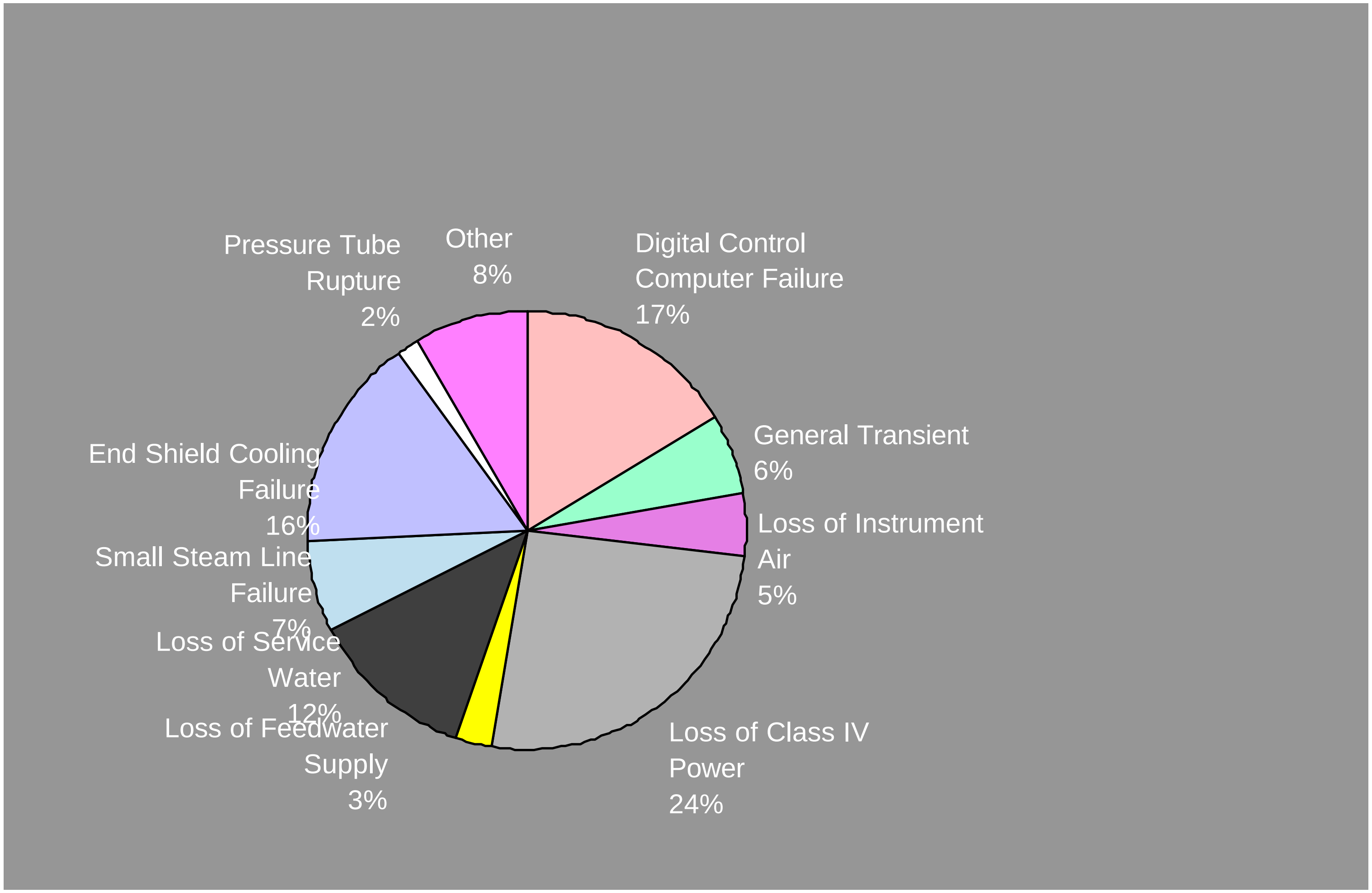
Nuclear Power Plants - Mitigating Systems

- **shutdown system #1**
- **shutdown system #2**
- **emergency core cooling system**
- **containment**
- **moderator**
- **shutdown cooling system**
- **auxiliary feedwater**
- **emergency (seismically qualified) water**
- **emergency electrical power**
- **OPERATOR!!**
- **etc.**

Results of Risk Analysis

- Types of Risk Analysis:
  - Level 1 - Severe Core Damage / Core Melt Frequency
  - Level 2 - Frequency of Large Release
  - Level 3 - Frequency of Health Effects
- CANDU severe core damage frequency:
  - $\sim 10^{-5}$ per year for existing plants
  - $\sim 10^{-6}$ per year for new designs
- WASH-1400 for existing LWRs:
  - core melt frequency = 2×10^{-4} per reactor-year [since reduced]
  - frequency of large release = 10^{-6} per reactor-year

Severe Core Damage for CANDU 6



Conclusions

- **risk analysis is a way of predicting the hazard from *rare* events**
- **it is excellent at ranking technologies and looking at relative risks**
- **there are some uncertainties in absolute predictions:**
  - **adequacy of component failure data**
  - **have we got all the cross-links?**
  - **human performance models**
- **it allows rational decision making on safety**
  - **most effective allocation of safety resources**