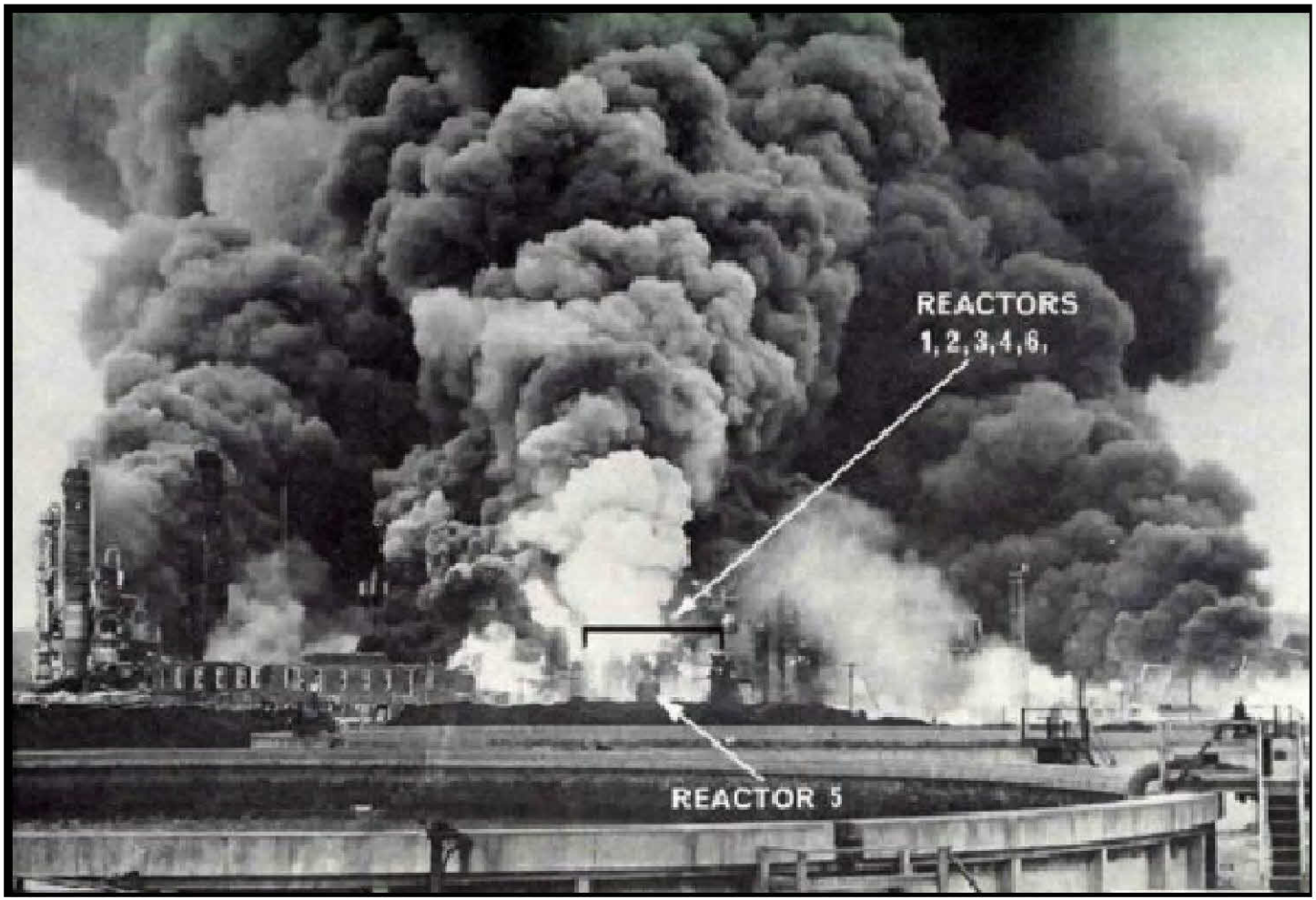
Design and Safety of Canadian Nuclear Reactors

Dr. V.G. Snell
UNENE Programme Director
Adjunct Professor, Engineering Physics, McMaster University
-and -
President, VGSSolutions

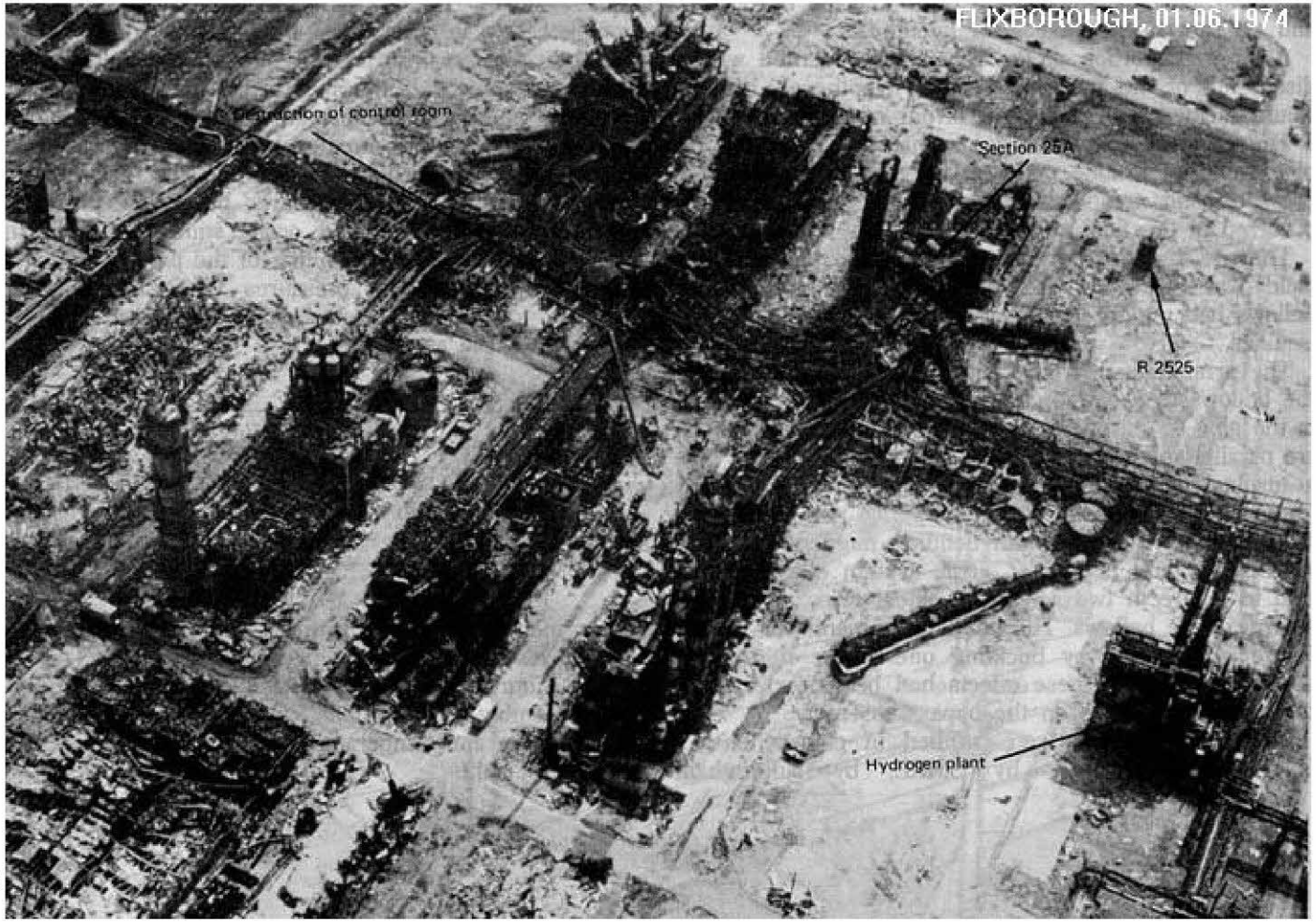
What Accident Was This?

- 28 workers killed, 36 injured
- Hundreds of off-site injuries
- 1800 homes & 167 businesses destroyed or badly damaged
- 16T TNT equivalent

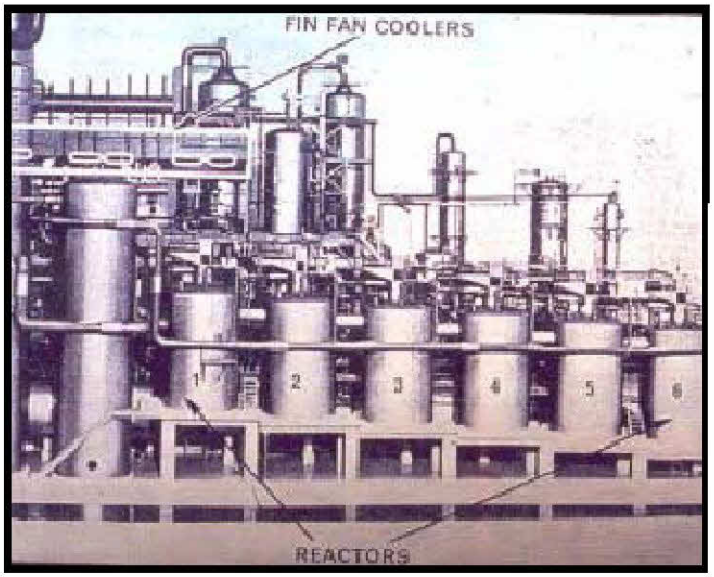
Ground-Level Photo

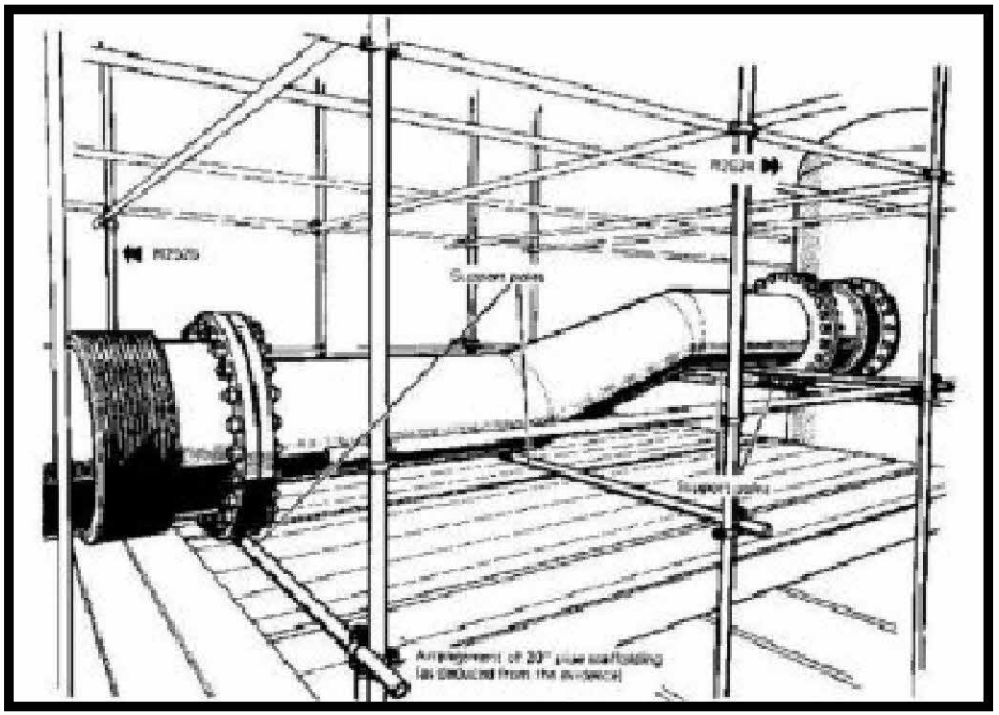


Aerial Photo



Design Authority?



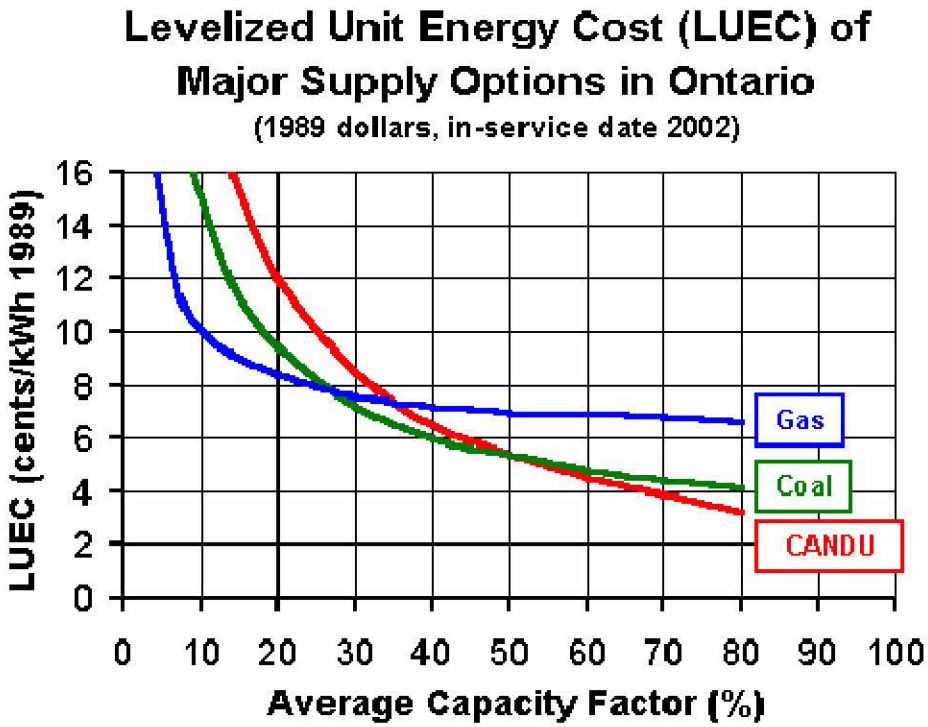


Outline

1. Why Reactors?
2. Reactor Design
3. Hazard
4. Safety Functions
5. Engineering Principles for Safety
   - Redundancy, Diversity, Separation
6. Severe Accidents
   - Three Mile Island
   - Chernobyl
   - Fukushima
7. CANDU design for severe accidents

Why New Reactors in Ontario?

- No emissions causing acid rain, smog, CO_2
- Safe – no major accidents in CANDUs
- Reliable – Darlington >90% capacity factor
- Economic compared to fossil fuels
- Current nuclear generation ~50% of Ontario electricity

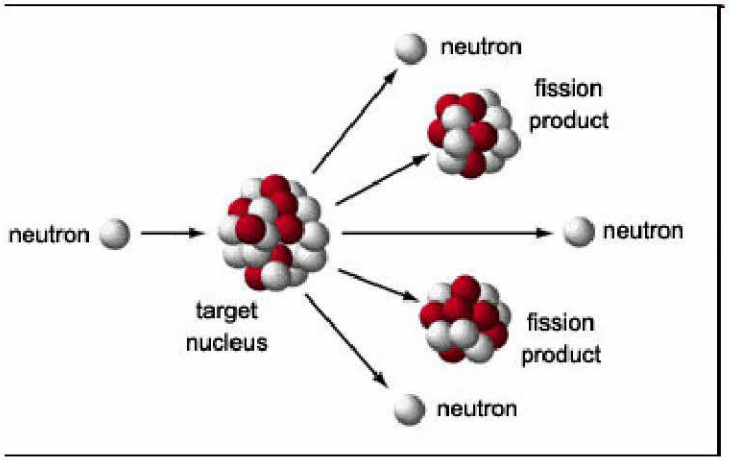


Darlington Environmental Assessment

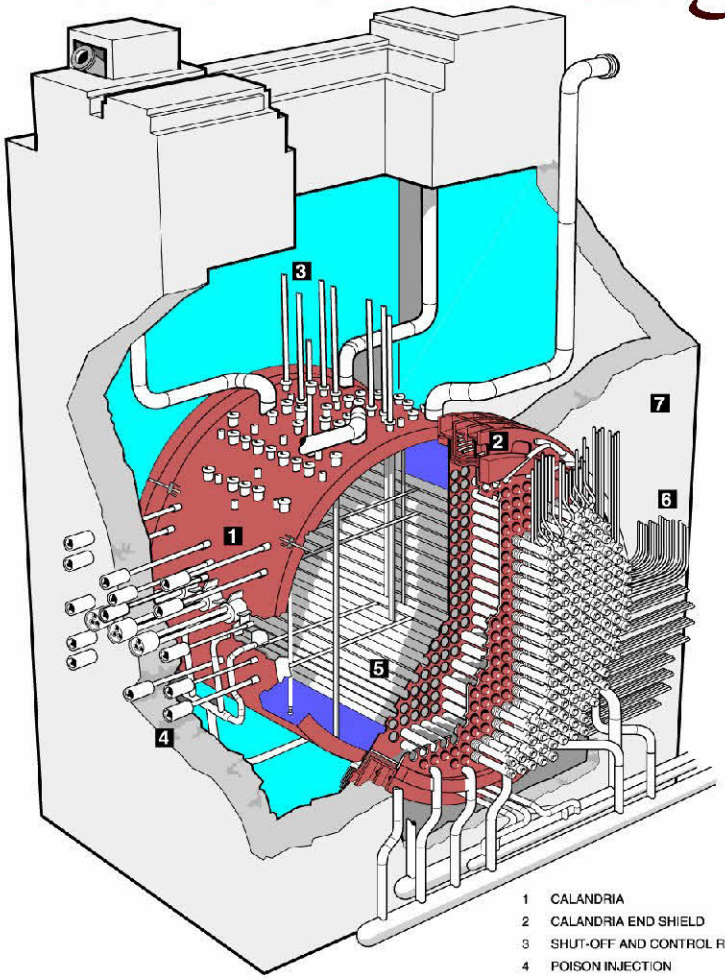
- Lengthy & thorough EA hearings
- Joint Review Panel: “The Panel concludes that the Project is not likely to cause significant adverse environmental effects, provided the mitigation measures proposed and commitments made by OPG during the review, and the Panel’s recommendations are implemented.”

What is a Nuclear Reactor?

- A geometrical arrangement of fuel, moderator, coolant and control devices
- Turns otherwise useless mineral (uranium) into heat
- Heat is used to make electricity, as in a conventional thermal plant
- Fission of 1 uranium-235 atom → 200MeV
  - Enough to move a grain of sand
- 1 gram of natural uranium contains ~2 x 10^{19} fissionable atoms



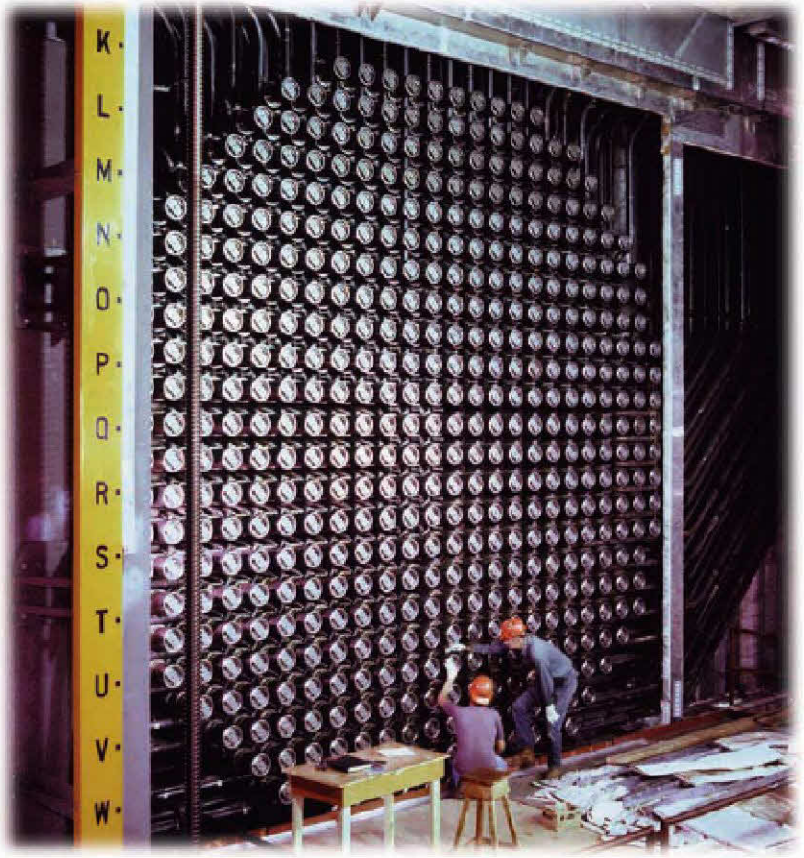
CANDU Design



1 CALANDRIA
2 CALANDRIA END SHIELD
3 SHUT-OFF AND CONTROL RODS
4 POISON INJECTION
5 FUEL CHANNEL ASSEMBLIES
6 FEEDER PIPES
7 VAULT

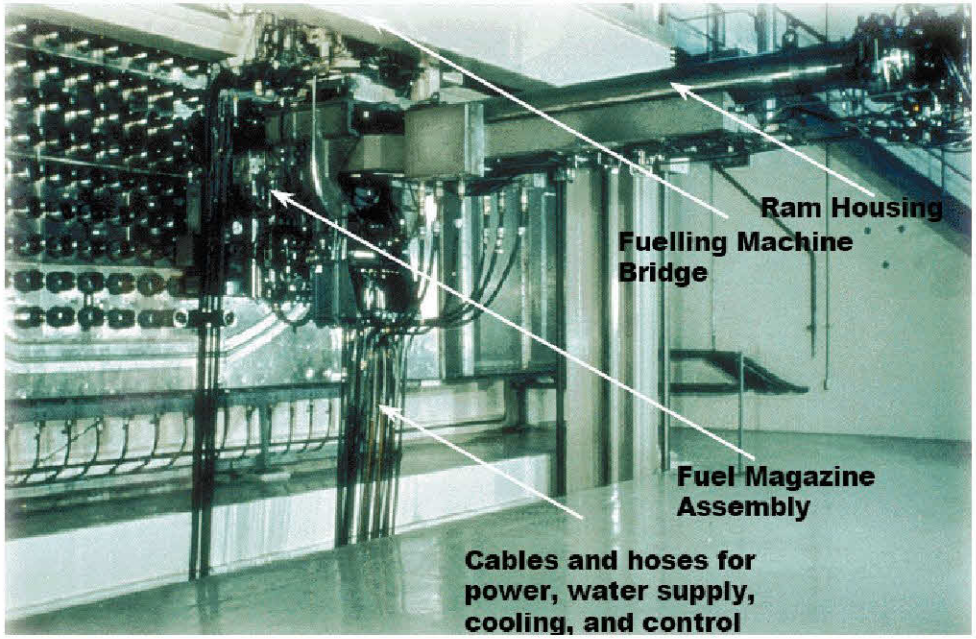
970667-2

CANDU 6 Reactor Assembly



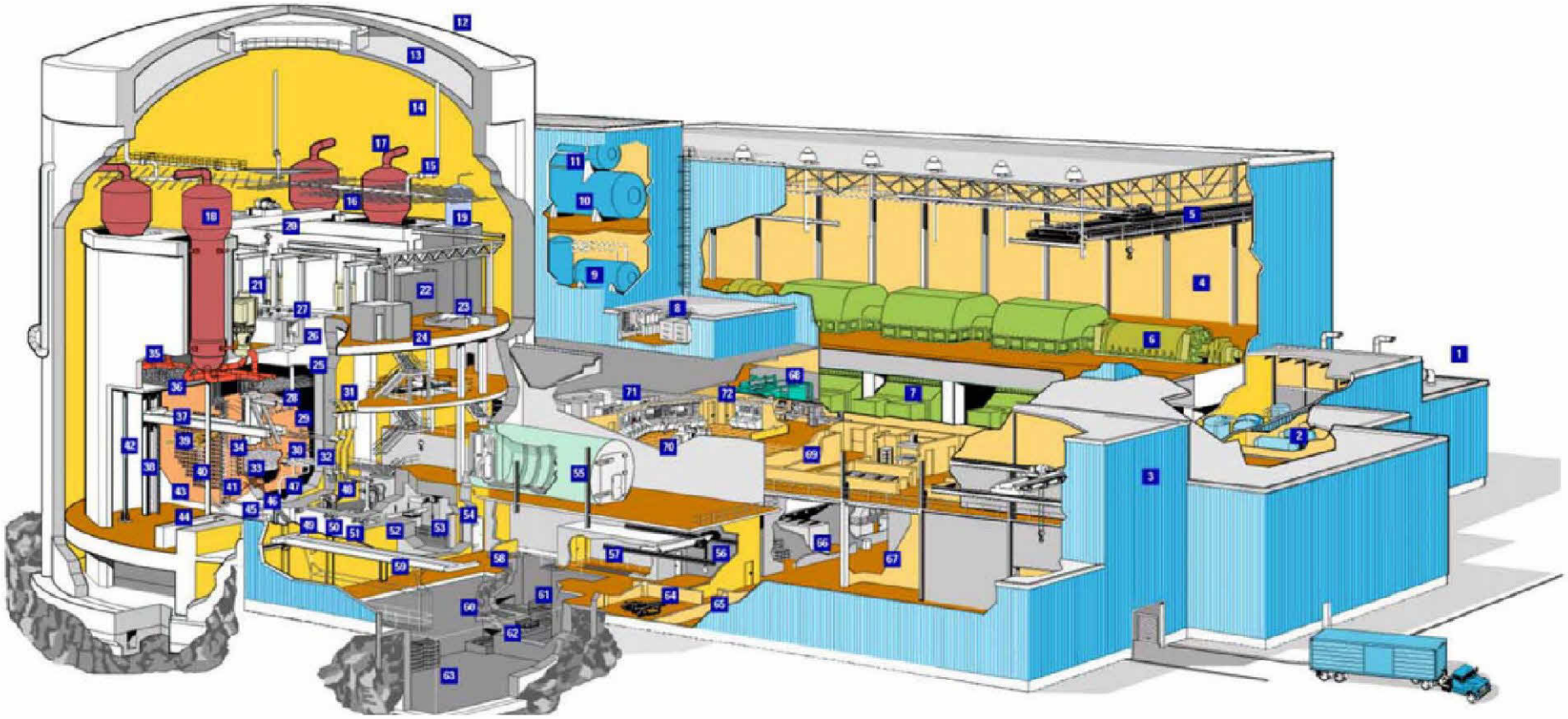
On-power refuelling

- Remote, by robot
- Visits about 2 channels per day
- Removes 4-8 bundles of used fuel and replaces it with new fuel

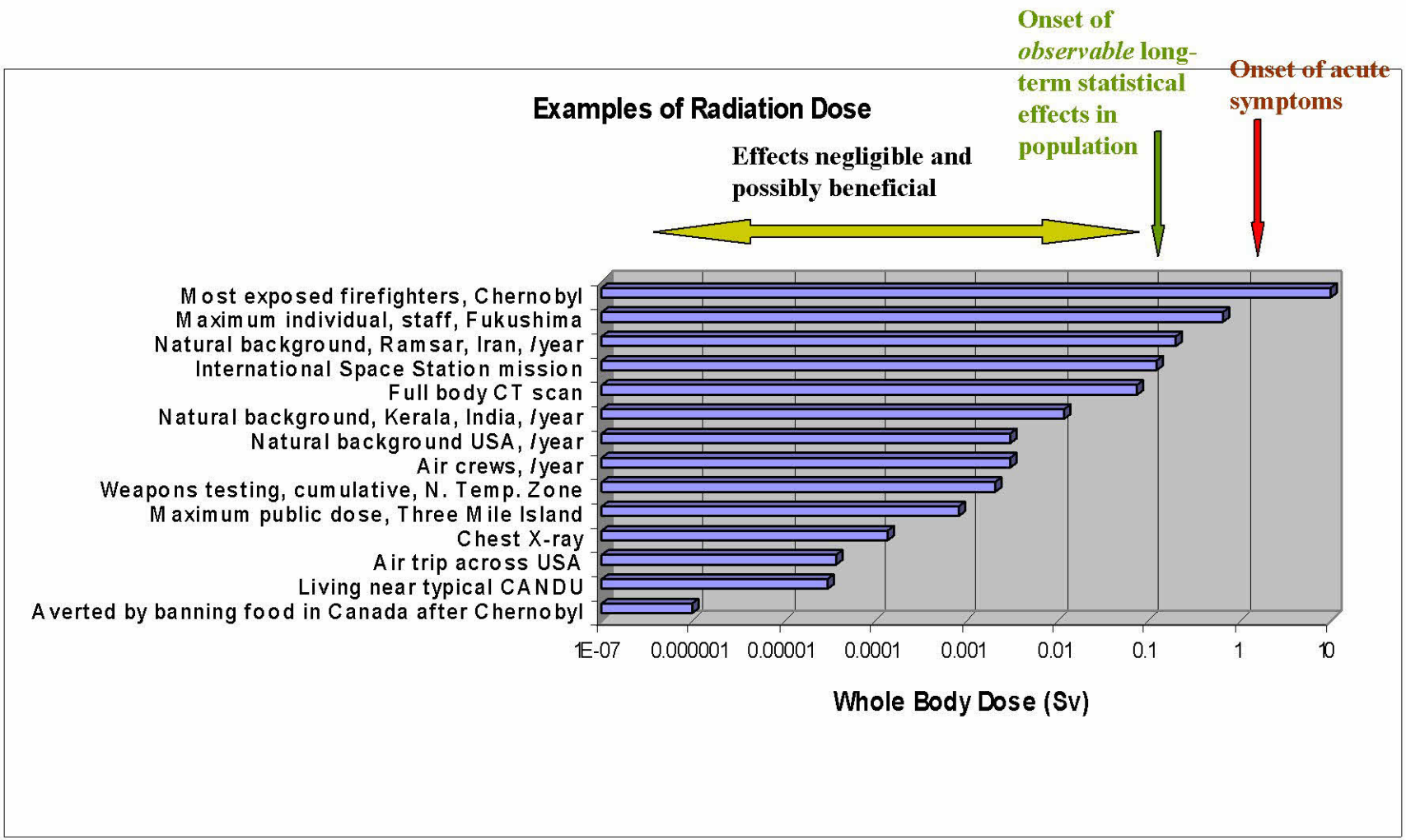


Fuelling Pickering Nuclear Plant

Heat to Electricity



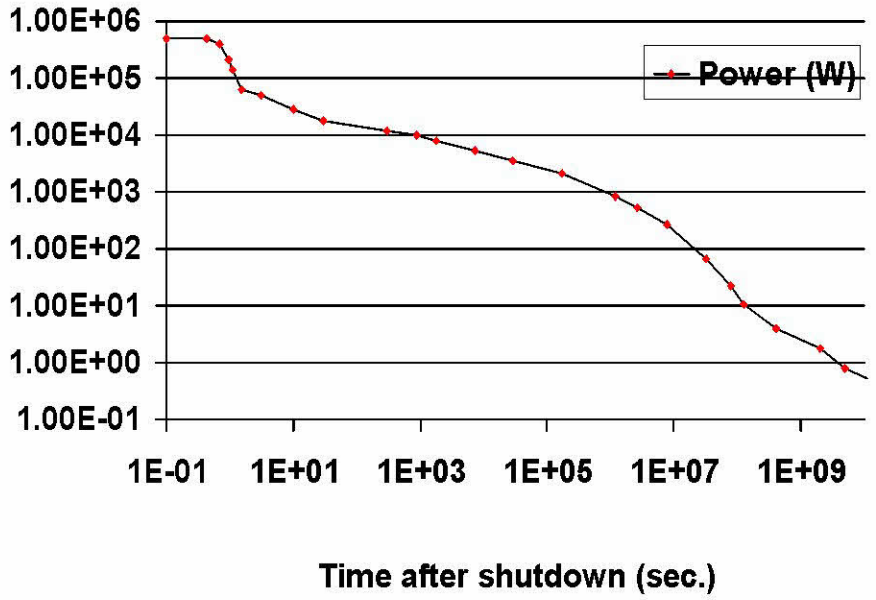
Hazard


Examples of Radiation Dose
Onset of *observable* long-term statistical effects in population
Onset of acute symptoms
Effects negligible and possibly beneficial
Most exposed firefighters, Chernobyl
Maximum individual, staff, Fukushima
Natural background, Ramsar, Iran, /year
International Space Station mission
Full body CT scan
Natural background, Kerala, India, /year
Natural background USA, /year
Air crews, /year
Weapons testing, cumulative, N. Temp. Zone
Maximum public dose, Three Mile Island
Chest X-ray
Air trip across USA
Living near typical CANDU
Averted by banning food in Canada after Chernobyl
1E-07
0.000001
0.00001
0.0001
0.001
0.01
0.1
1
10
Whole Body Dose (Sv)

Goal of reactor safety

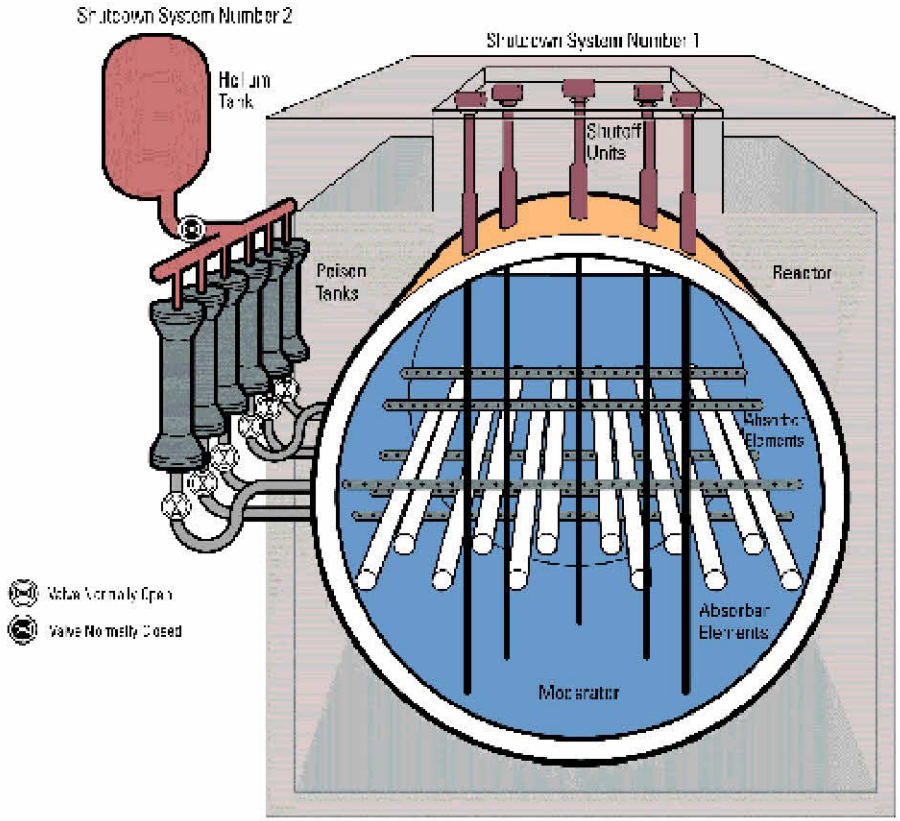
- To prevent unwanted movement of radioactivity
- Safety functions:
  - Shutdown
  - Cool
  - Contain
  - Monitor

CANDU Bundle Power after Shutdown



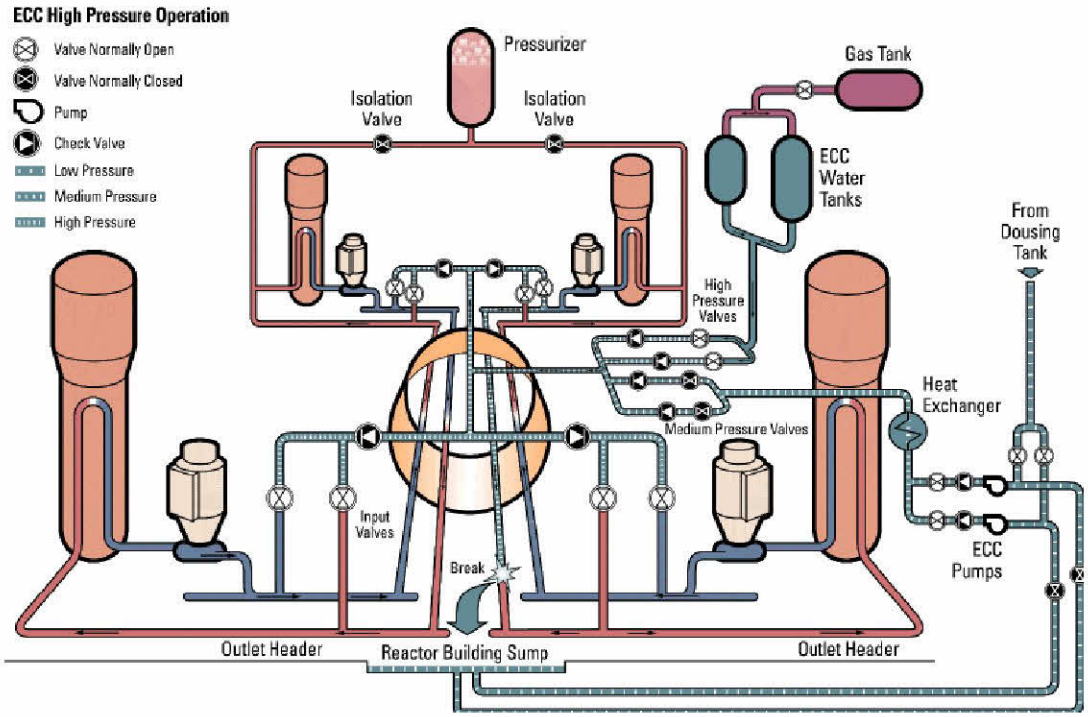
Shutdown – Two Systems + Control

- Insert neutron-absorbing material quickly into the moderator (<2 seconds)
- Rods from top (by gravity), or liquid under pressure
- "Passive" once actuated
- Fail-safe on loss of power



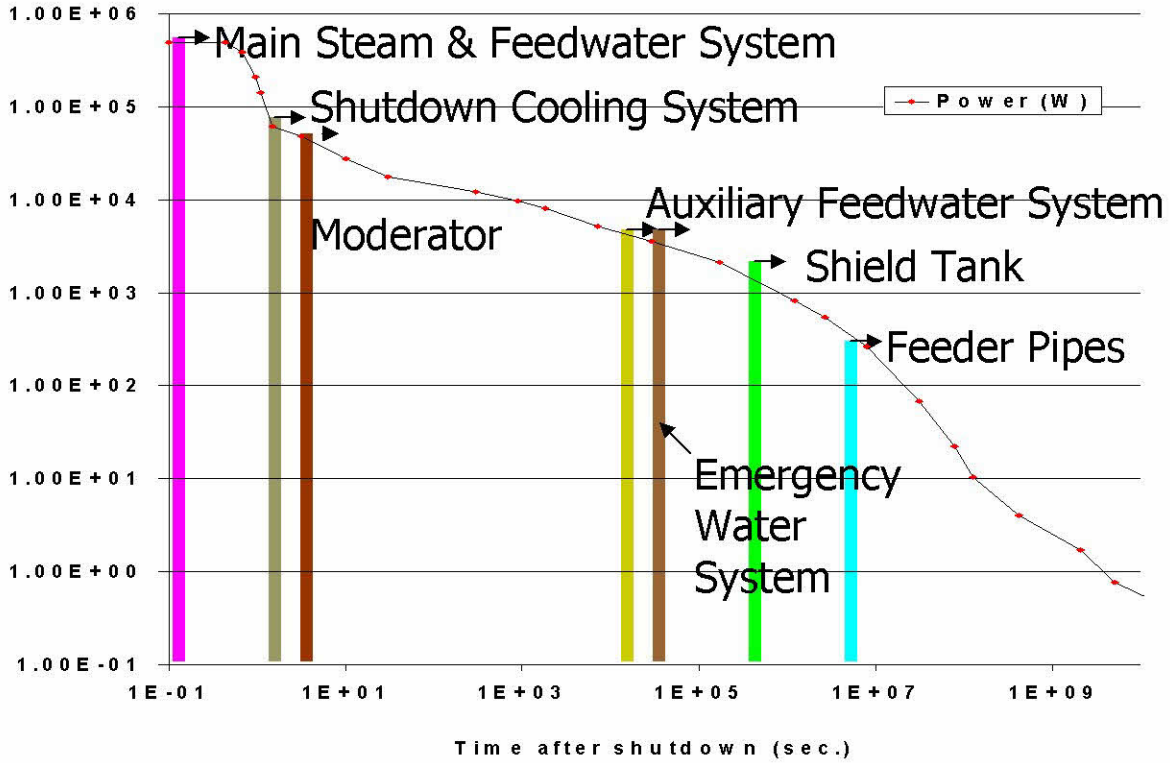
Cool

- Injection of water if a coolant pipe breaks (Emergency Core Cooling)
- Heat removal via pumps and heat exchangers to ultimate heat sink



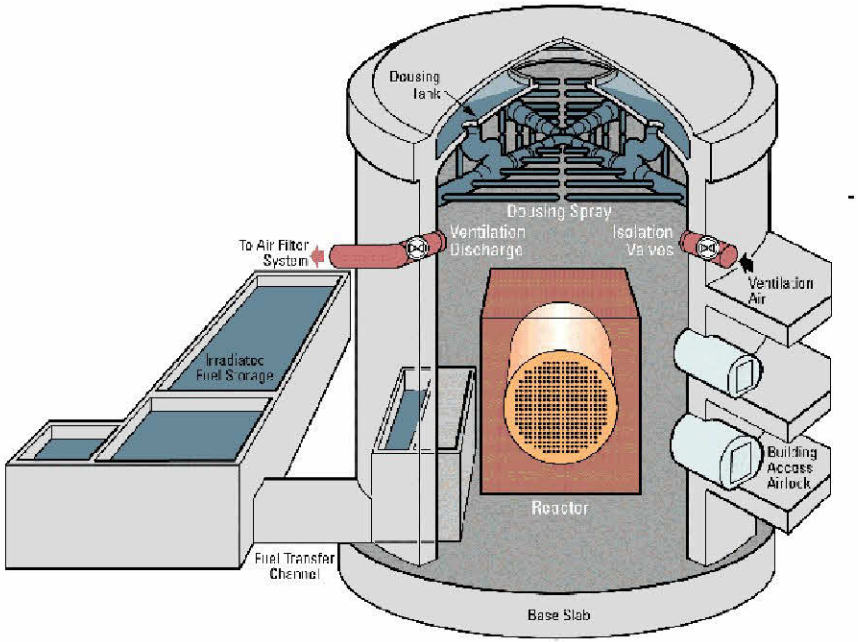
Many systems can remove decay heat

CANDU Bundle Power after Shutdown



Contain

- Barrier to escape of radioactivity
- Barrier to external events & malevolent acts



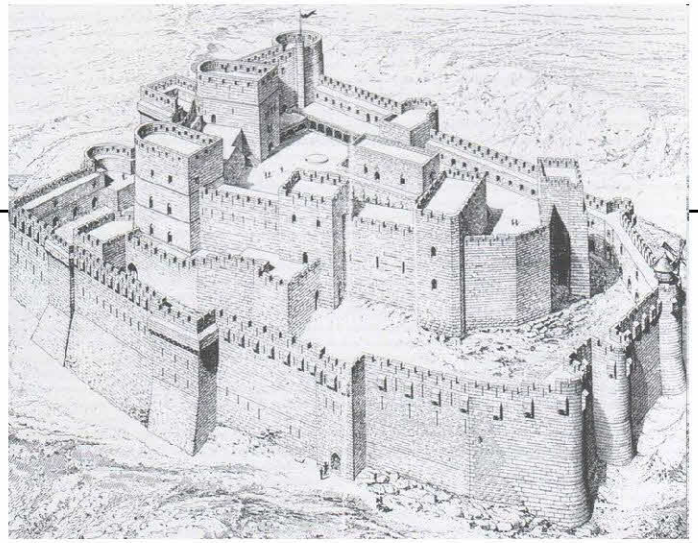
Monitor

- Two separated control rooms
- Main Control Room for normal operation and most accidents
- Secondary Control Area for accidents

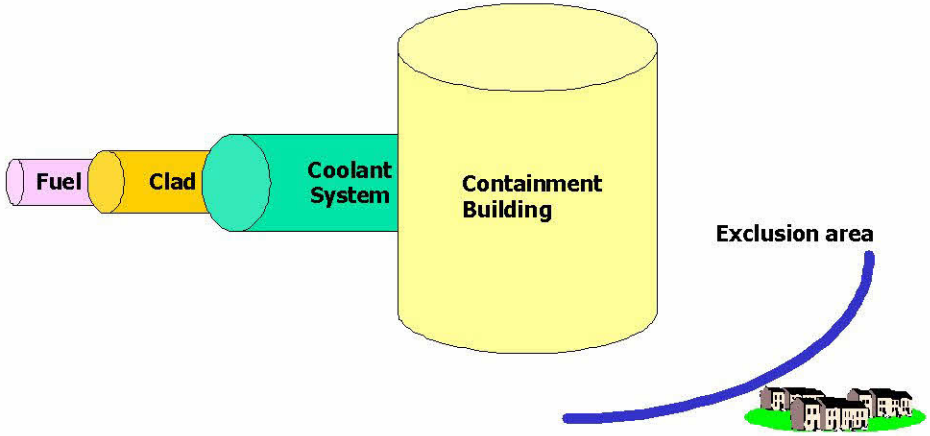
Darlington Main Control Room

Defence in Depth

- Protect via overlapping series of barriers
- Failure of one barrier does not lead to disaster
- A nuclear power plant need not be perfect to be safe



Krak des Chevaliers, Syria



Other Principles

Concept

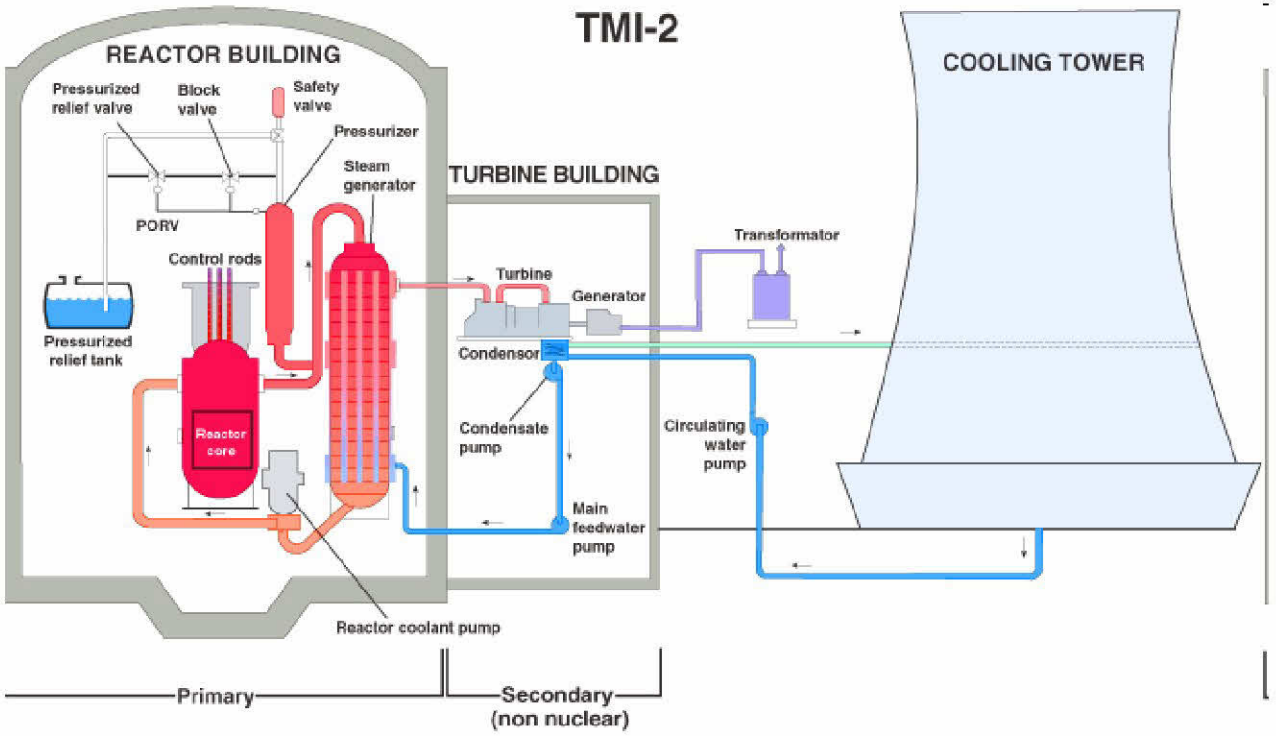
- Redundancy
  - System level, component level
- Diversity
- Separation
  - Geometric, barriers
- Reliability
  - Test during operation

Examples

- Control system + two shutdown systems
- Rods vs. liquid, different manufacturers
- Two safety groups, each capable
- 99.9% availability for each safety system

Three Mile Island – Loss of Coolant

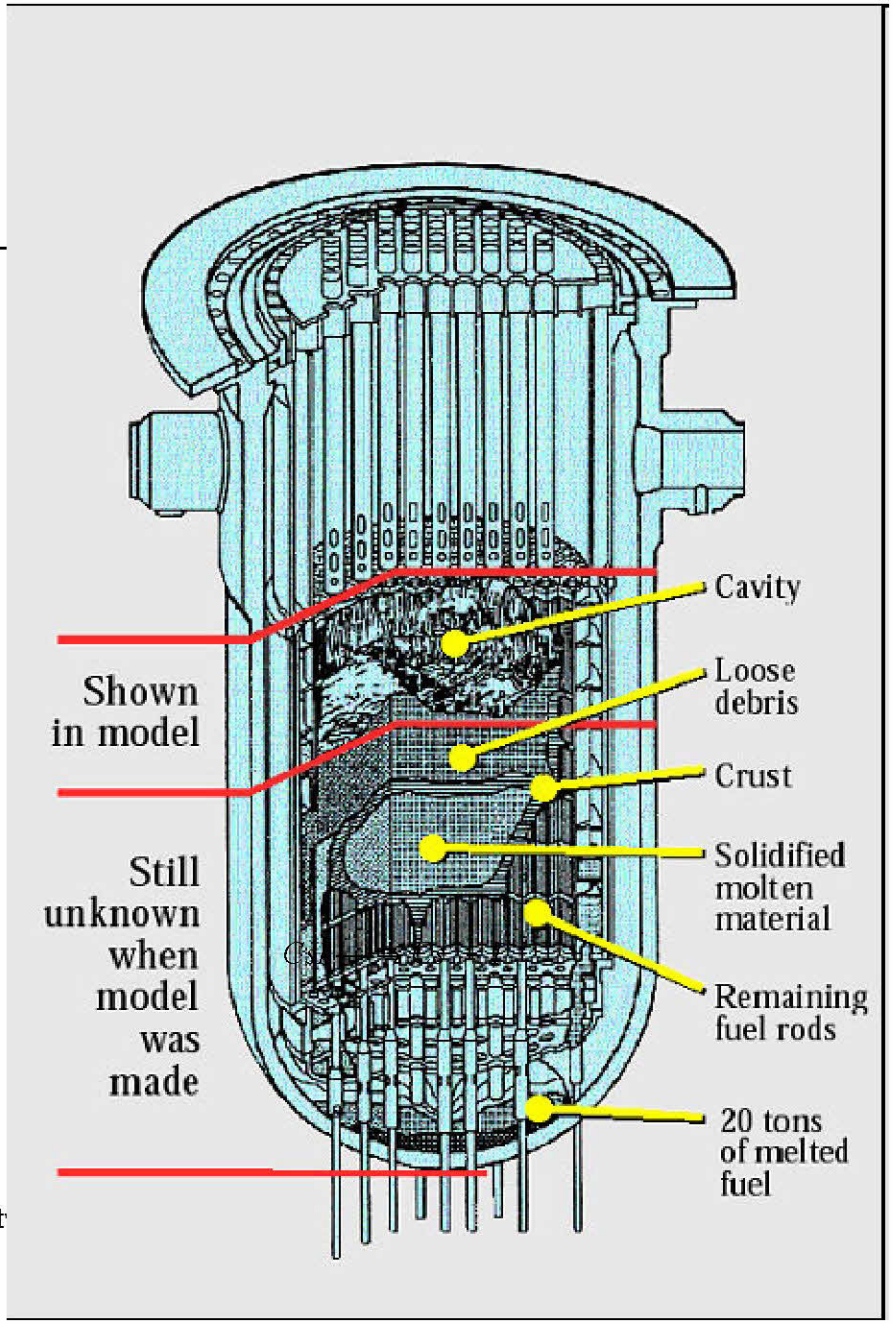
- Failure of relief valve to close
- Mis-diagnosed
- Resulted in small loss of coolant for hours
- Partial core melt
- Reactor vessel intact
- Releases very small with no health consequences



TMI – cont'd

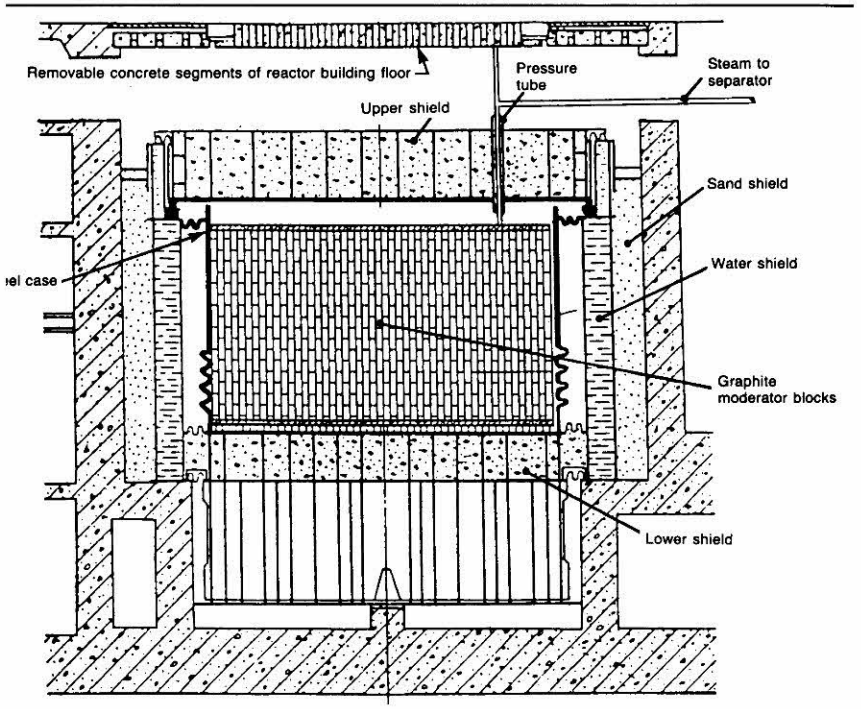
- Design of valve position indicators
- Operator training / aids
- Hydrogen control
- Primary Coolant Pumps
- Revise prescriptive approach
- Severe Accidents – PSA
- Wetter is better

$$CsI \longrightarrow Cs^{+} + I^{-}$$



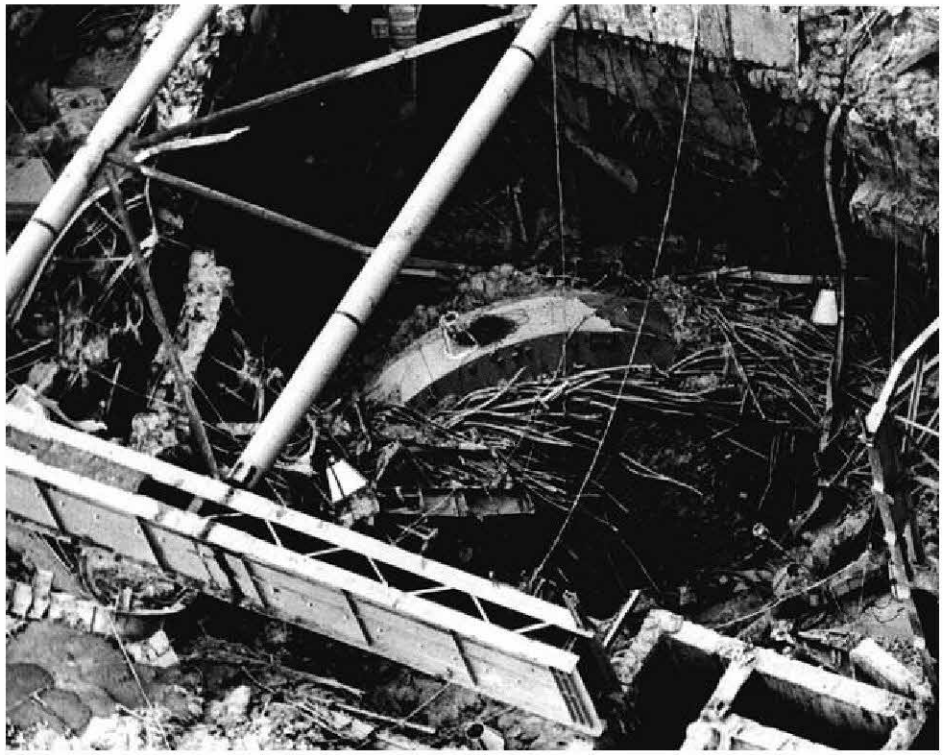
Chernobyl – Loss of Control

- Light-water cooled
- Direct cycle
- Vertical pressure tubes
- Graphite moderator
- Positive power feedback which *depended on reactor state*



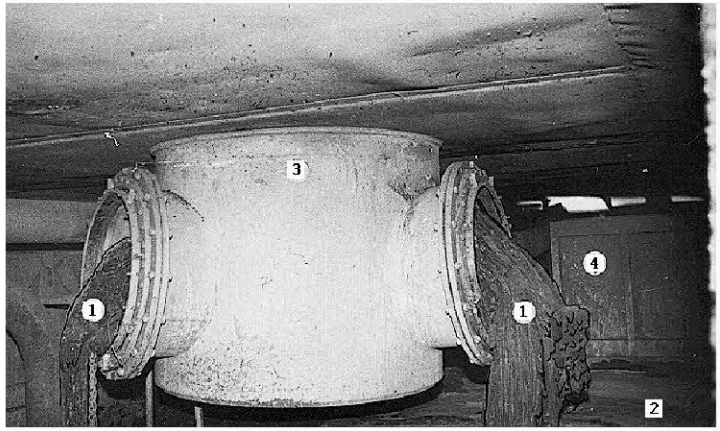
Accident Sequence

- Test to show that a running-down turbine could power main pumps
- Reactor & pump trip at low power with core near boiling
- Power rise due to positive feedback
- Accelerated by reverse action of shutoff rods
- Fuel vaporization, steam explosion
- Ejection of core lid



Accident Sequence - 2

- Massive core destruction / dispersal – subcritical
- Graphite fire for several days
- Core melted and ‘lava’ flowed into rooms below reactor; core area empty

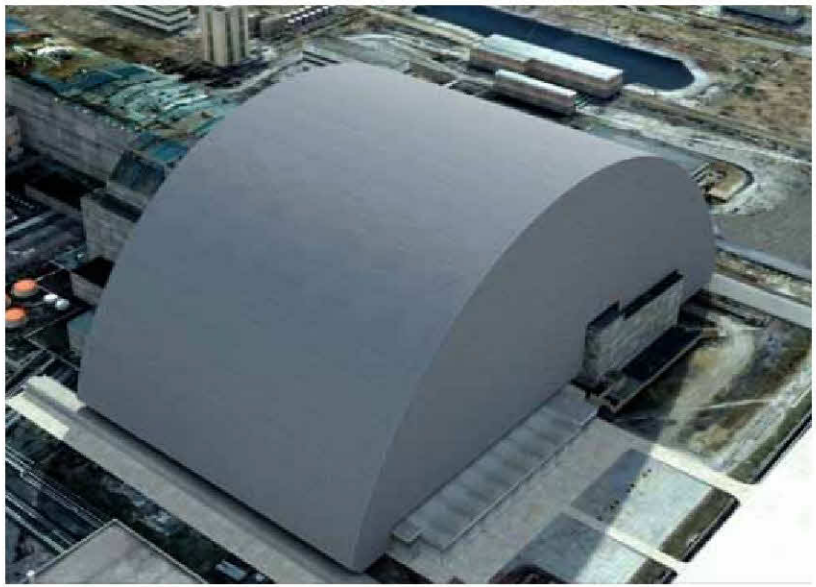


Consequences

- 31 prompt deaths (operators, firefighters)
- Delayed cancers:
  - Few thousand excess thyroid cancers observed, mostly in children – mostly curable
  - There is no evidence of other radiation induced cancers in the three most contaminated countries at this time.
  - Death rate of all "liquidators" *less* than in comparable population

Lessons learned

- Lack of robust design of (single) shutdown system
  - Reactor was never designed nor intended to be operated at low power with boiling coolant
- Test procedure subject to ad hoc alteration
- Lack of questioning attitude → ***Safety culture***

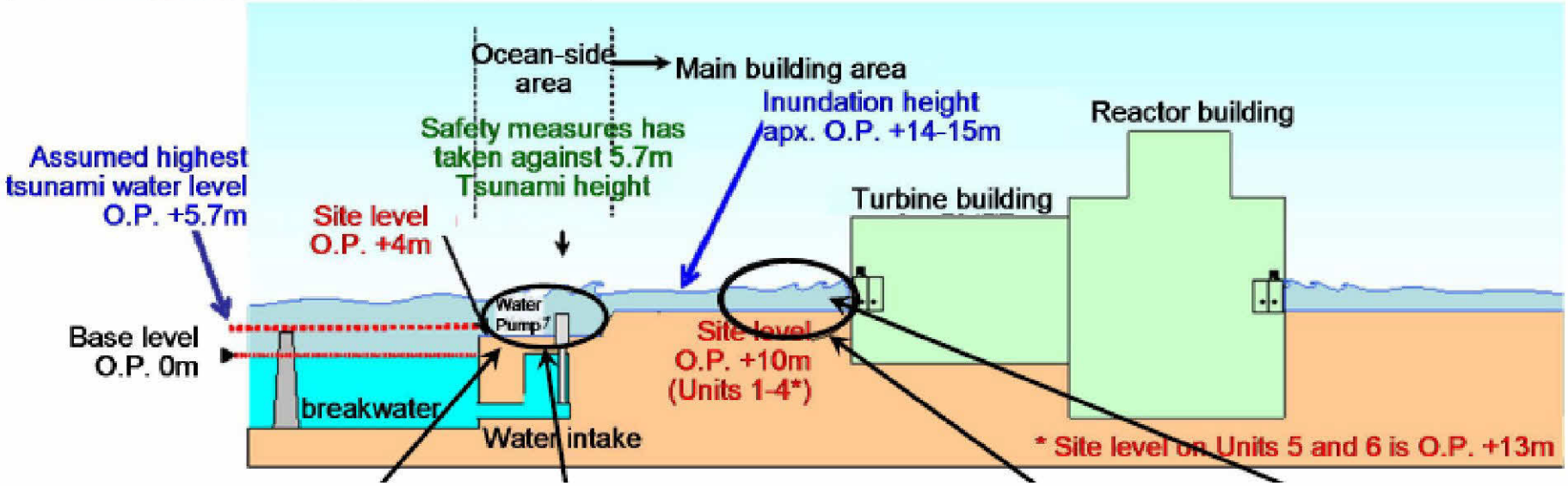


Future plans

Fukushima – Loss of Heat Removal

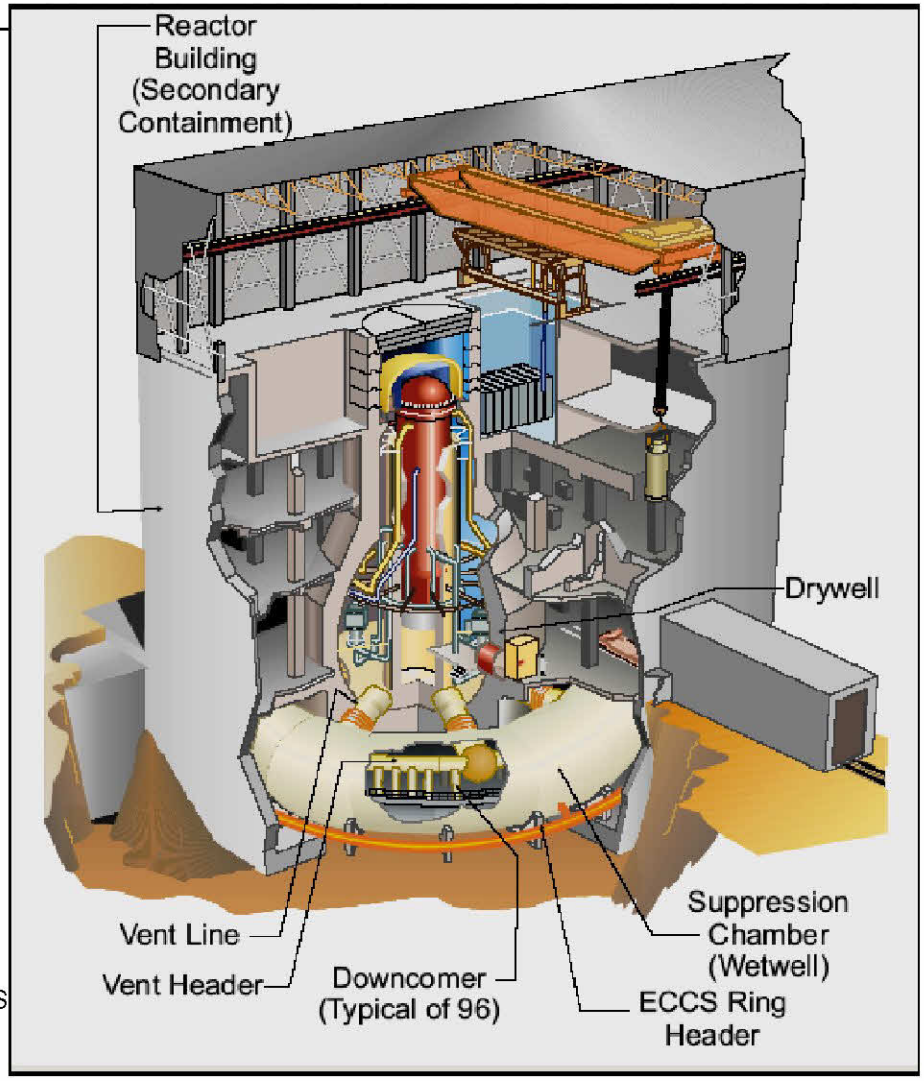
- Magnitude 9 earthquake off east Japan coast
- Caused 14m. high tsunami at Fukushima 40 minutes later
- Plant shut down & survived earthquake well
- Tsunami caused loss of all electrical power

Key safety equipment flooded



With no heat removal …

- Water in vessel boils away
- Steam condenses in suppression pool & heats it up
- Fuel uncovered
- Hydrogen produced
- Pressure in containment (wet-well) increases



Challenges and Responses

Challenges

- Restore water over the fuel
- Prevent containment failure due to over pressure
- Control and release the hydrogen

Responses

- Firewater & seawater injection to reactor
- Containment venting
- ...but too late - extremely difficult working conditions

Likely Consequences

- Fuel in Units 1, 2, and 3 melted a few hours after uncovery, and may have penetrated the reactor vessel
- Containment is damaged
- Fuel in two spent fuel bays not significantly damaged; other two unknown
- Inferred from calculations and some measurements, not known with certainty

Health Effects

- Based on published doses to workers, unlikely to see any long-term effects on staff
- 20km. evacuation zone
  - stable iodine
  - early sheltering from 20 to 30 km.
  - voluntary evacuation from 20 to 30 km.
- No authoritative calculations released to date for actual and projected public dose
  - Expect << Chernobyl

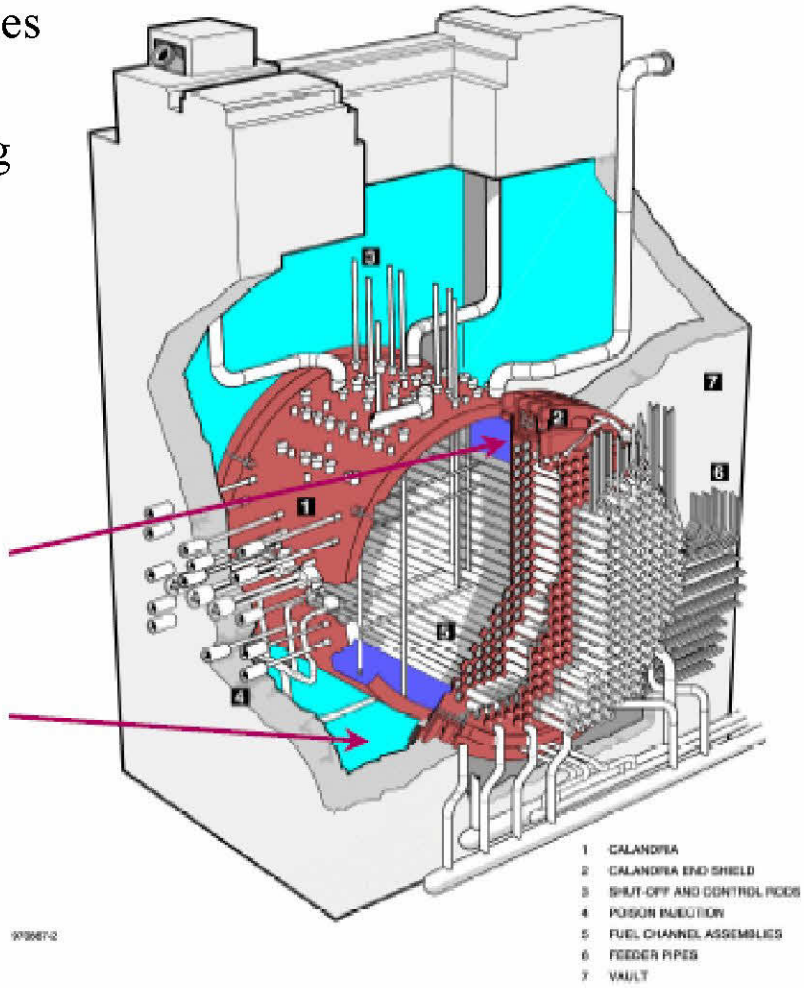
Some Lessons Learned

- Completeness of design basis
- Length of on-site coping time after severe accident
- Spent fuel bay cooling
- Continued monitoring
- Batteries – mission time
- Accident management after physical destruction and high radiation fields
- Role of regulator / government
- Effect of multiple units
- World-wide reviews and actions

CANDU Severe Accident Heat Removal

- Large water volumes near the fuel give long times to passively boil off
- As long as moderator tank is full, loss of cooling water over the fuel does not result in core melt
- Can be topped up
- Severe accidents happen slowly in CANDU

System	*Continuous Heat Removal Capability (% Full Power)*	*Time to Heat Up and Boil Off, Passive Heat Removal Only*
Moderator	**4.4%**	**> 5 hours**
Shield Tank	**0.4%**	**10-20 hours**



With loss of all heat removal

LWRs

- Fuel melts rapidly (tens of minutes) and "candles" down to the bottom of the vessel
- Vessel fails suddenly ejecting molten fuel
- Potential for steam explosion in vessel and in containment

CANDU

- Fuel melts slowly (hours) and slumps gradually down to the bottom of the vessel
- Vessel fails after a day; shield tank provides further barrier
- Continual steam release - explosion less likely

Conclusions

- Design and operating lessons learned from three severe accidents over last 32 years
  - But core melt is not the health disaster it was once thought to be
- CANDU safety design stacks up well to these challenges
- Post-Fukushima changes taking advantage of inherent CANDU features (e.g. topping up moderator) will make CANDU more robust