Canadian Nuclear Safety Commission | Commission canadienne de sûreté nucléaire

Canadian Nuclear Safety Commission

Presentation to the University of Ottawa
December 04, 2015

François Rinfret, ing.
Director,
Darlington Regulatory Program Division

Presentation designed by S. Eisan, DRPD staff

CNSC CCSN

nuclearsafety.gc.ca

e-Doc 4892574

Canada

Introduction

- François Rinfret
- B. A. Sc. (Mechanical Engineering) 1981
- Currently Director at the CNSC

Presentation Overview

- Introduction
- CNSC - Overview
- Safety and Control Areas
- Refurbishment of Darlington NGS
  - Gentilly-2 GS, Point-Lepreau GS, Bruce NGS
- Focus on Mech. and Elec. Engineering
  - Thermodynamic Cycle, Materials, Pumps, Motors, Systems
  - Electrical Distribution

Presentation Overview

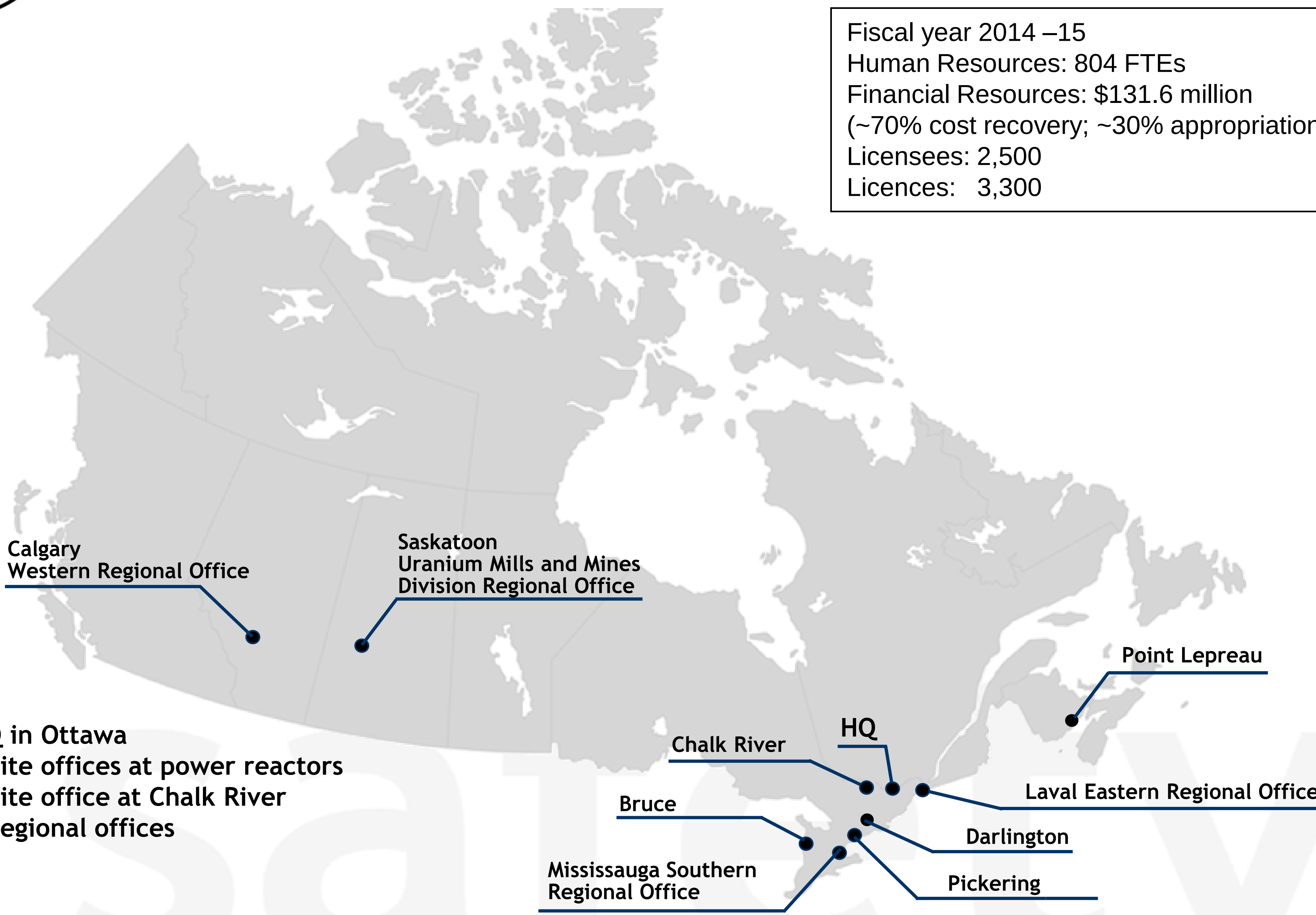
- Design principles for CANDU
  - Redundancy, Safe Failure, Triplication (channelization), Diversity, Independence
  - Defense in Depth
  - Others: Simple, Passive
- Fukushima Enhancements
- Learning from Events
  - 3-Mile island, Tchernobyl, Davis-Besse,
  - Mégantic
- Discussion

Overview

- The Canadian Nuclear Safety Commission (CNSC) is:
  - Canada's nuclear watchdog
  - A quasi-judicial body
  - Independent of, but not isolated from government
- The CNSC regulates the use of nuclear energy and materials to protect the health, safety and security of Canadians and the environment; to implement Canada's international commitments on the peaceful use of nuclear energy; and to disseminate objective scientific, technical and regulatory information to the public.

Overview – CNSC across Canada

Fiscal year 2014 –15
Human Resources: 804 FTEs
Financial Resources: $131.6 million
(~70% cost recovery; ~30% appropriation)
Licensees: 2,500
Licences: 3,300



HQ in Ottawa
4 site offices at power reactors
1 site office at Chalk River
4 regional offices

Regulatory Approach

- Licensing regime from begining to end
- Licensee responsible for Safety
- CNSC: Establishing Standards and Controls
- Verification for Compliance:
  - Inspections
  - Event reviews
  - Documents review
  - Review of performance indicators
  - Following technical files and corrective actions, to closure
- Report to Commission and Canadians

Safety and Control Areas

Management	Management System	Management System
		Organization
		Change Management
		Safety Culture
		Configuration Management
		Records Management
		Management of Contractors
		Business Continuity
	Human Performance Management	Human Performance Programs
		Personnel Training
		Personnel Certification
		Initial Certification Examinations and Requalification Tests
		Work Organization and Job Design
		Fitness for Duty
	Operating Performance	Conduct of Licensed Activity
		Procedures
		Reporting and Trending
		Outage Management Performance
		Safe Operating Envelope
		Severe Accident Management and Recovery
		Accident Management and Recovery

Safety and Control Areas

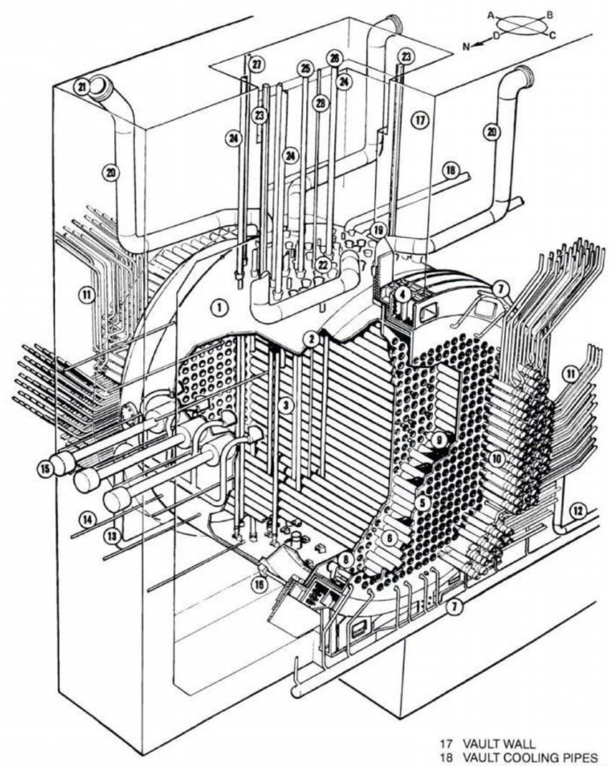
Facility and Equipment	Safety Analysis	Deterministic Safety Analysis
		Probabilistic Safety Analysis
		Criticality Safety
		Severe Accident Analysis
		Environmental Risk Assessment
		Management of Safety Issues
	Physical Design	Design Governance (includes EQ)
		Site Characterizations
		Facility Design
		Structure Design
		System Design
		Components Design
	Fitness for Service	Equipment Fitness for Service/ Equipment Performance
		Maintenance
		Structural Integrity (includes reliability)
		Aging Management
		Chemistry Control
		Periodic Inspection and Testing

Safety and Control Areas

Core Control Processes	Radiation Protection	Application of ALARA
		Worker Dose Control
		Radiation Protection Program Performance
		Radiological Hazard Control
		Estimated Dose to Public
	Conventional Health and Safety	Performance
		Practices
		Awareness
	Environmental Protection	Effluent and Emissions Control (releases)
		Environmental Management System (EMS)
		Assessment and Monitoring
		Protection of the Public
	Emergency Management and Fire Protection	Conventional Emergency Preparedness and Response
		Nuclear Emergency Preparedness and Response
		Fire Emergency Preparedness and Response
	Waste Management	Waste Characterization
		Waste Minimization
		Waste Management Practices
		Decommissioning Plans
	Security	Facilities and Equipment
		Response Arrangements
		Security Practices
		Drills and Exercises
	Safeguards and Non-Proliferation	Nuclear Material Accountancy and Control
		Access and Assistance to the IAEA
		Operational and Design Information
		Safeguards Equipment, Containment and Surveillance
	Packaging and Transport	Package Design and Maintenance
		Packaging and Transport
		Registration for Use

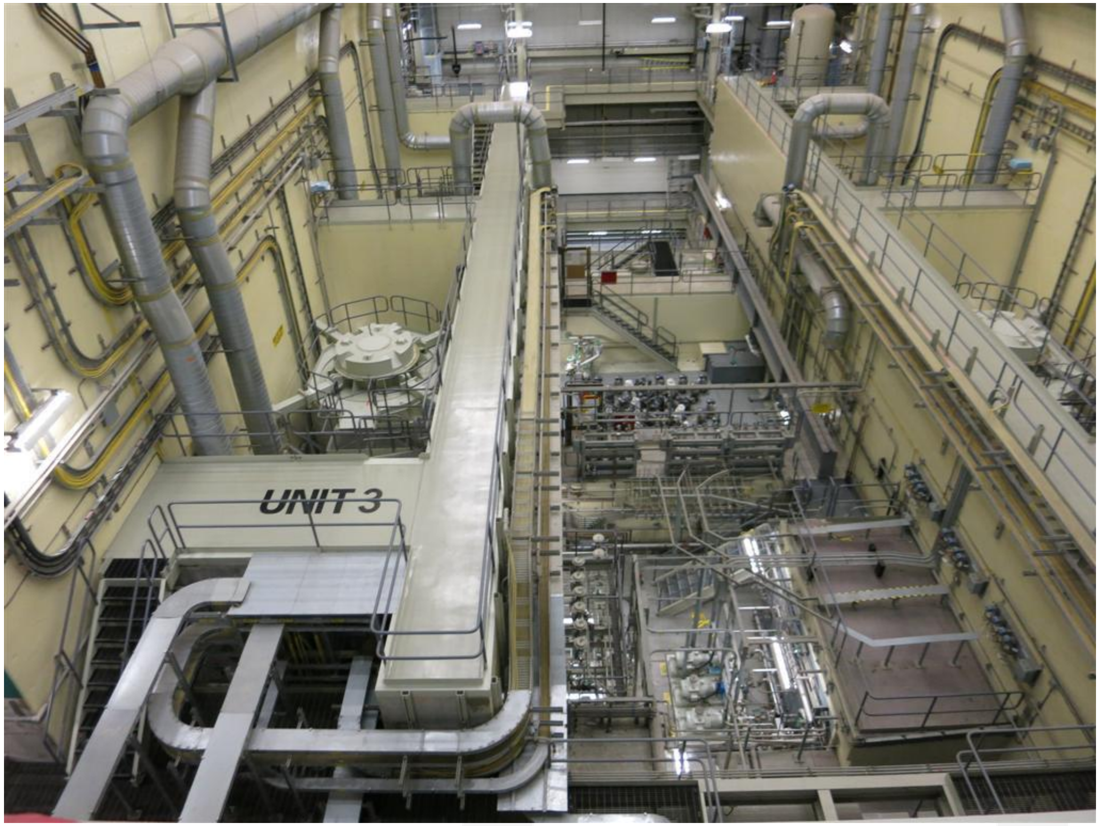
Darlington Nuclear Generating Station

Reactor Vault and Assembly



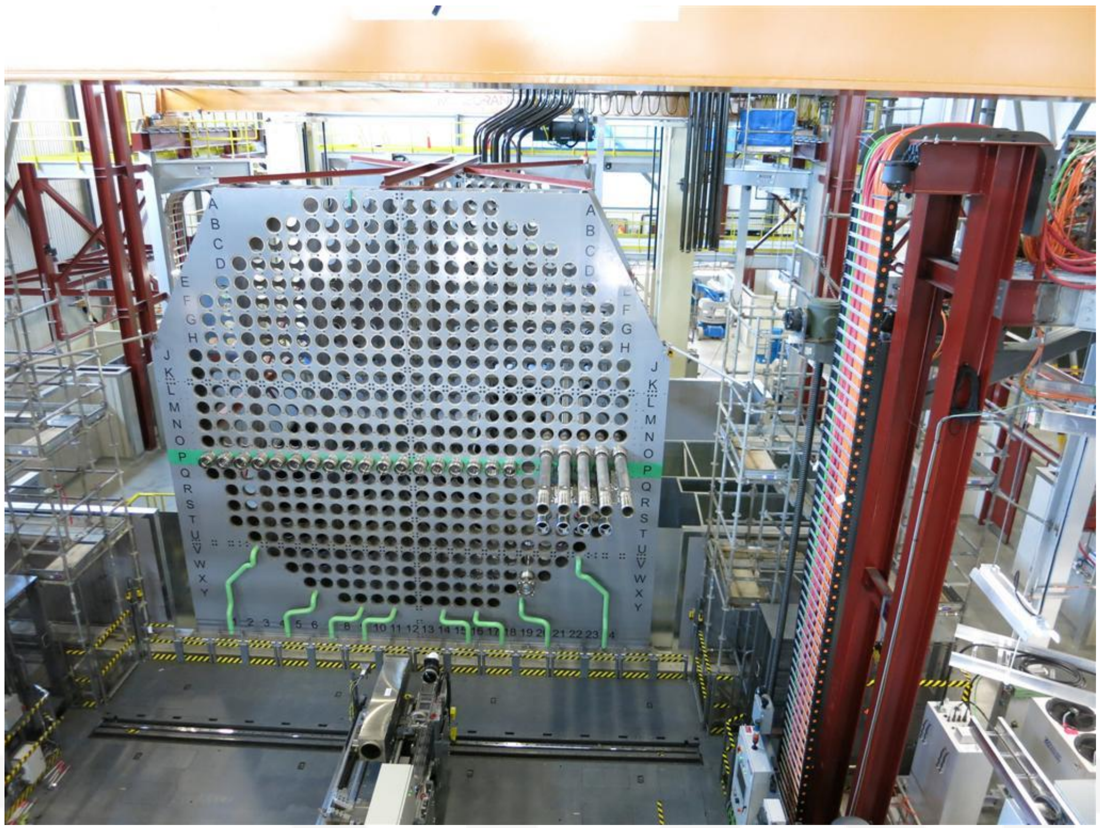
1 CALANDRIA
2 CALANDRIA SHELL
3 CALANDRIA TUBES
4 EMBEDMENT RING
5 FUELLING TUBESHEET
6 END SHIELD LATTICE
7 END SHIELD COOLING PIPES
8 INLET OUTLET STRAINER
9 STEEL BALL SHIELDING
10 END FITTINGS
11 FEEDER PIPES
12 MODERATOR OUTLET
13 MODERATOR INLET
14 FLUX MONITOR AND POISON INJECTION
15 ION CHAMBER
16 EARTHQUAKE RESTRAINT
17 VAULT WALL
18 VAULT COOLING PIPES
19 MODERATOR OVERFLOW
20 ACCIDENT DISCHARGE PIPE
21 RUPTURE DISC
22 REACTIVITY CONTROL ROD NOZZLES
23 VIEWING PORT
24 SHUTOFF ROD
25 ADJUSTER ROD
26 CONTROL ABSORBER ROD
27 ZONE CONTROL ROD
28 VERTICAL FLUX MONITOR

View of PHT Pump Motors and Reactivity Deck

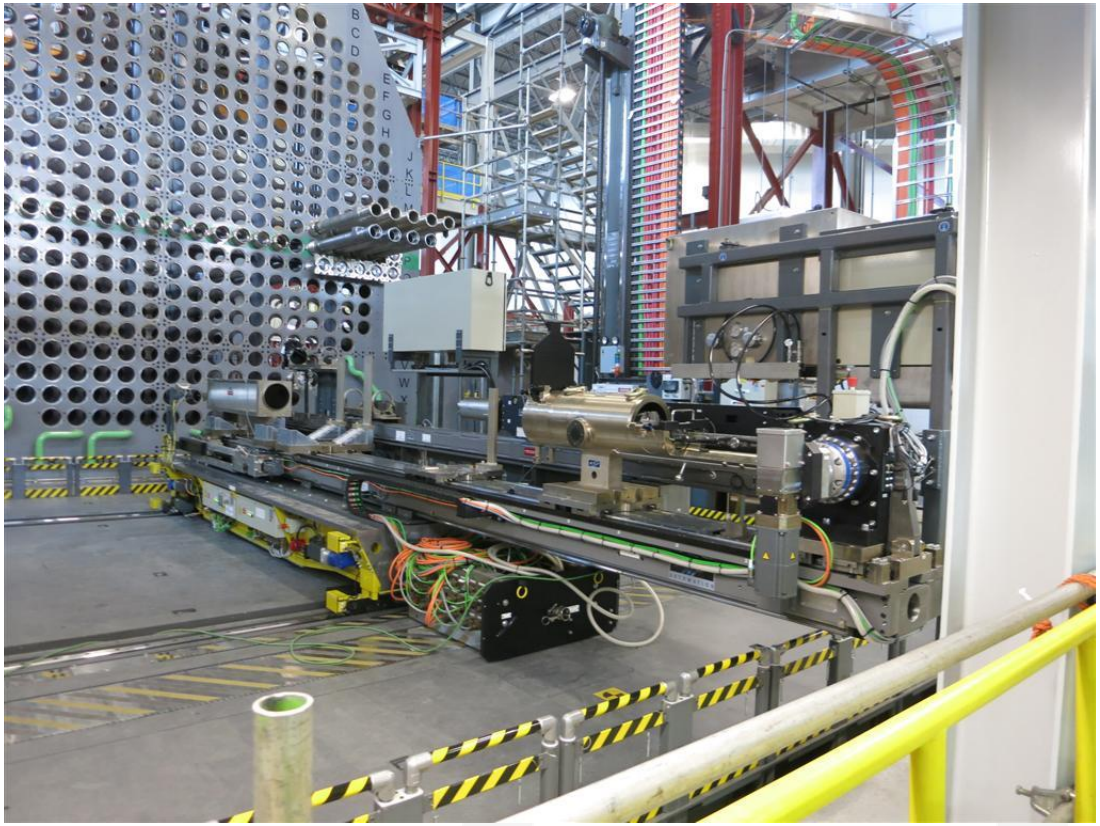


Spare PHT Pump Motor

Mock-up Facility

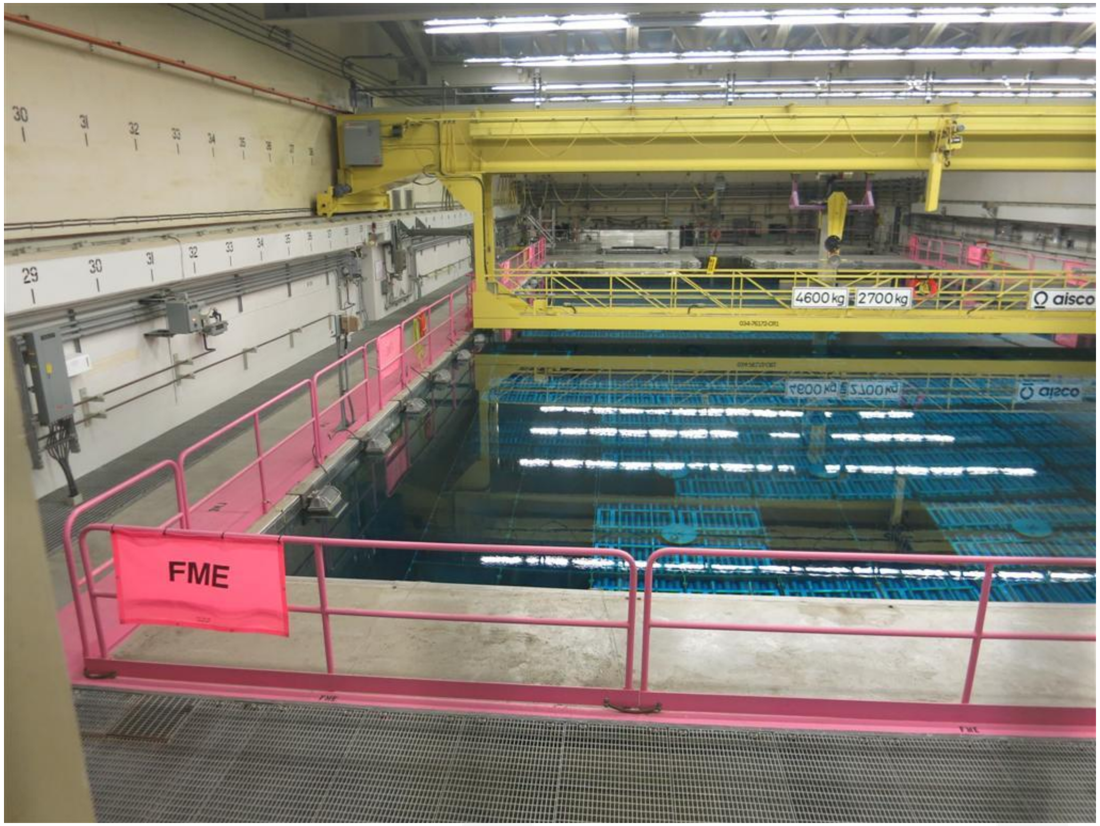


Tooling for Channel Replacement in Mock-up Facility

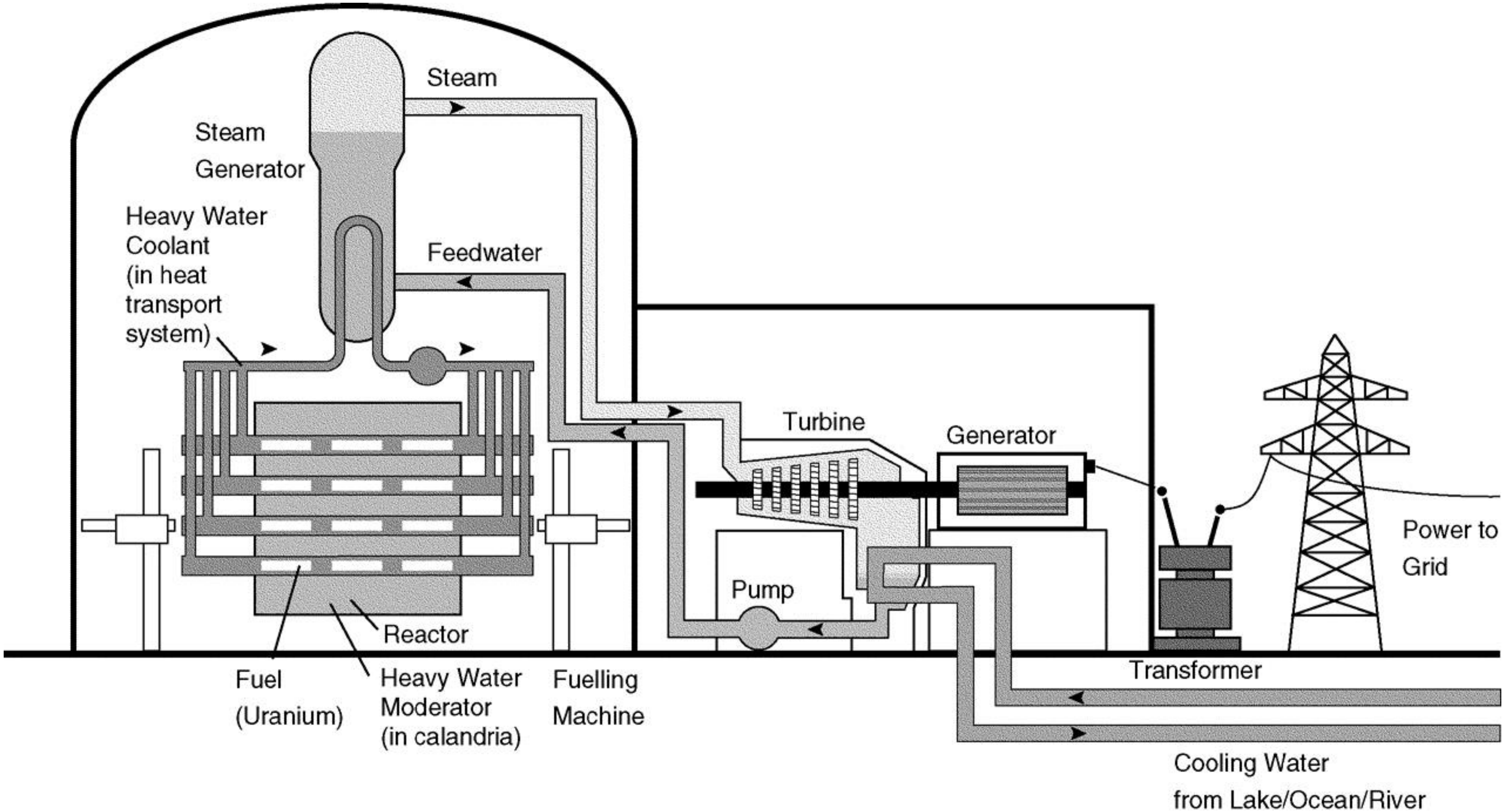


Turbine Bay (Unit 4, Unit 3)

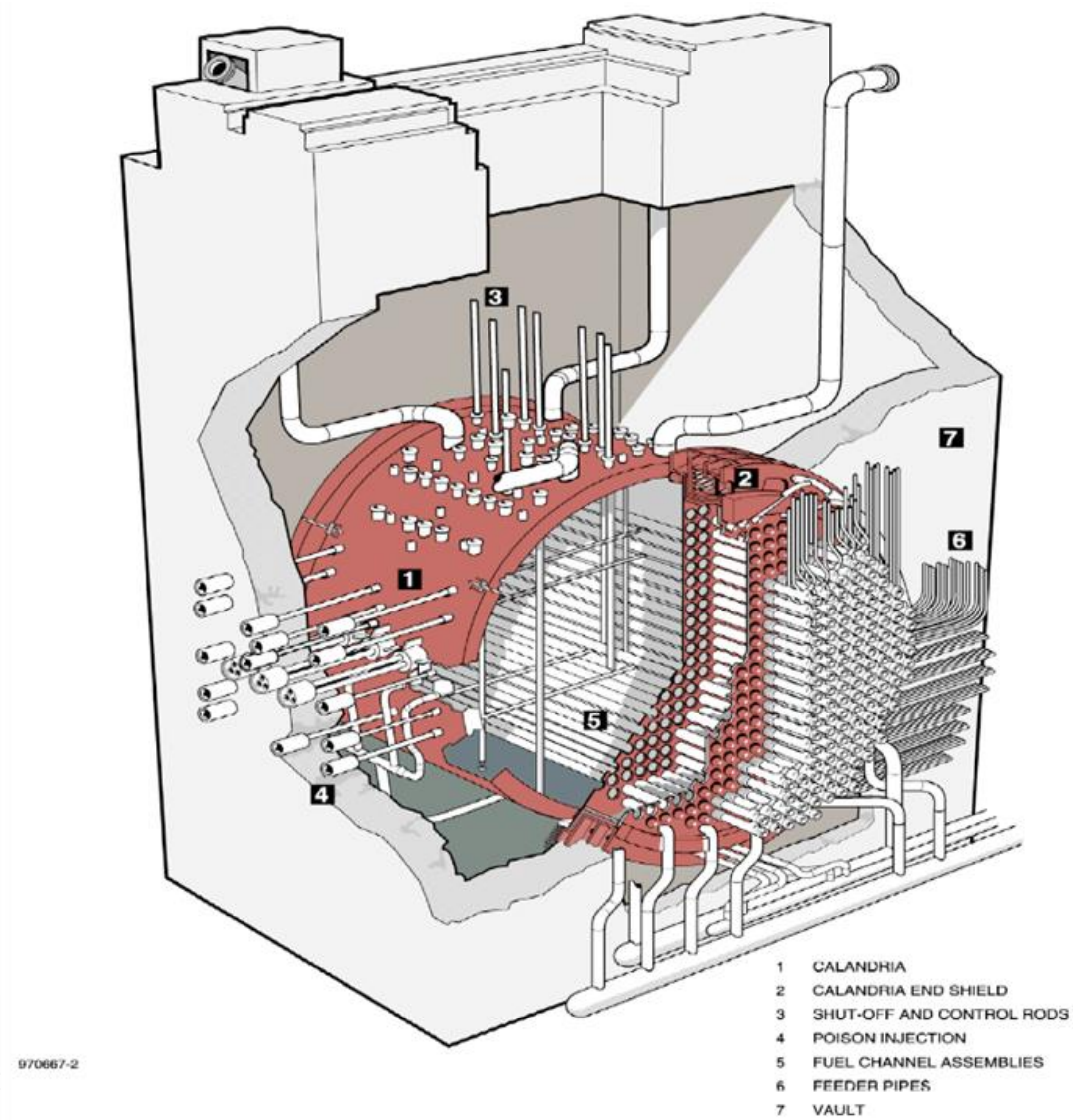
Irradiated Fuel Bay (East)



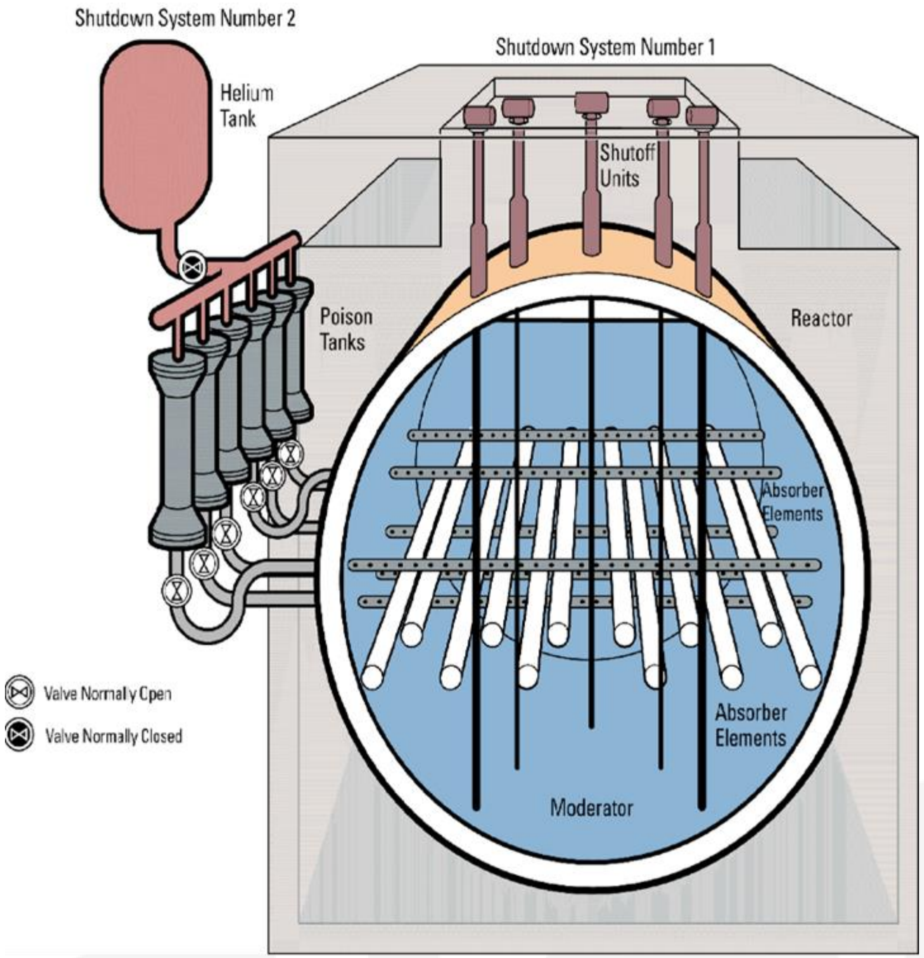
CANDU reactor



Shut Down System no 1

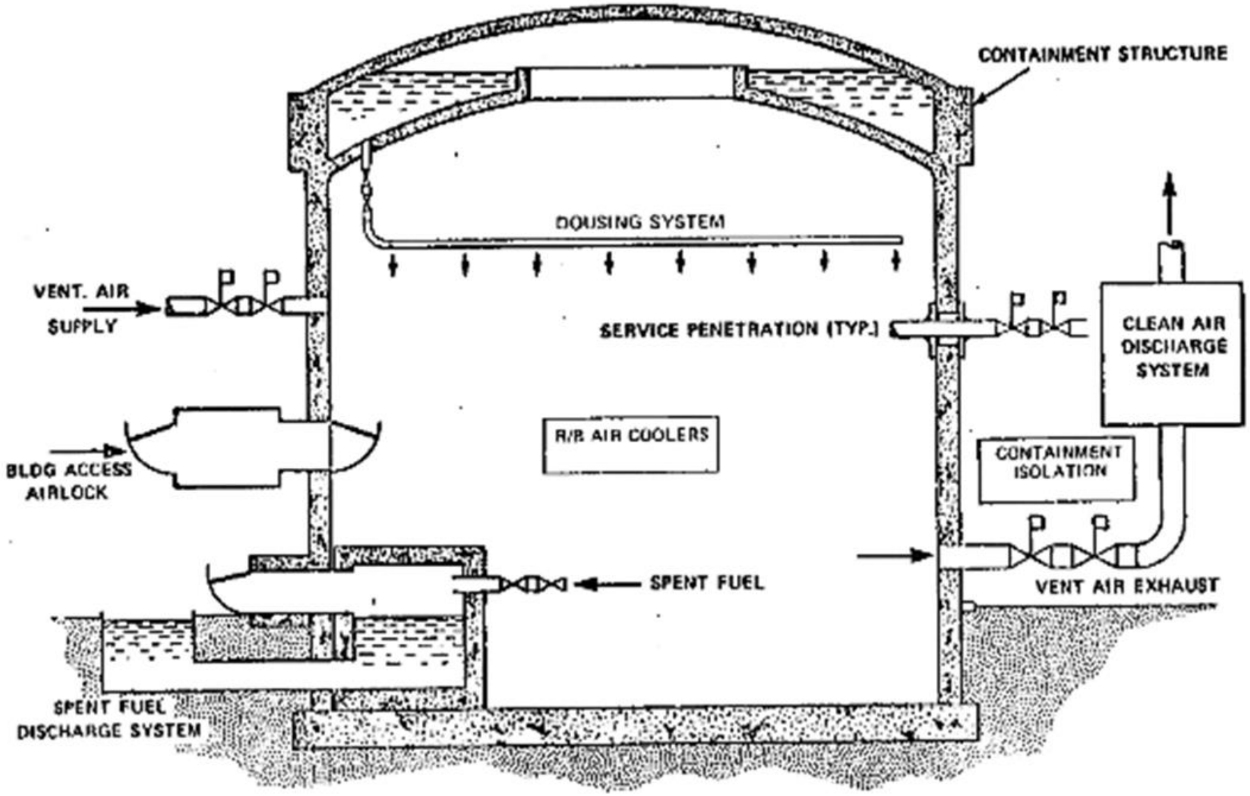


Shut Down System no 2

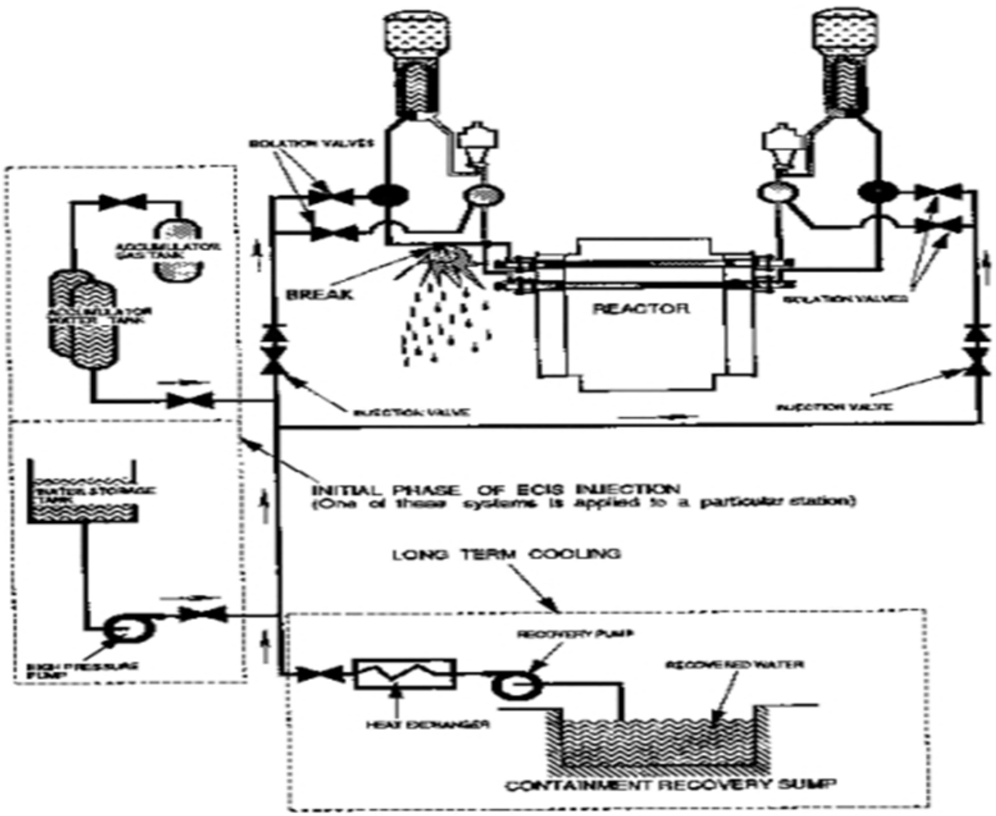


Nuclear Security

Containment system

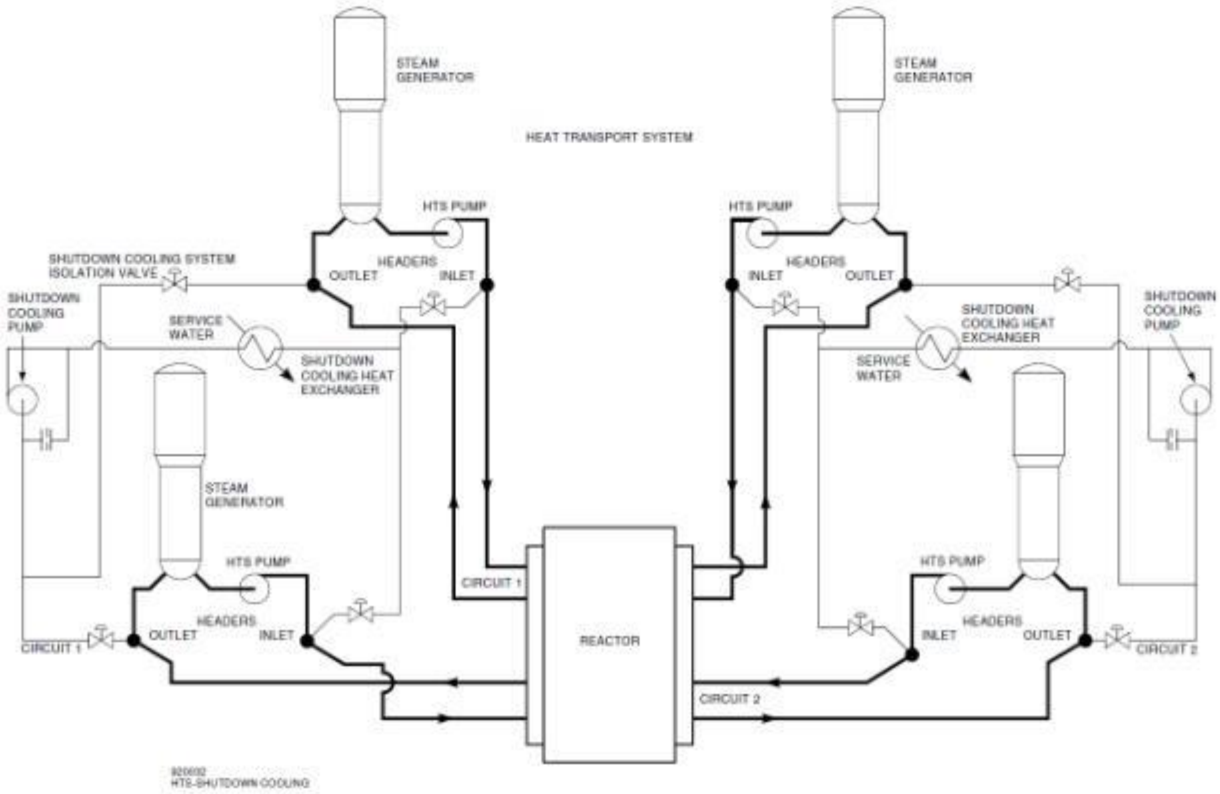


Emergency Core Injection



Calandria in transit

Heat Transport System



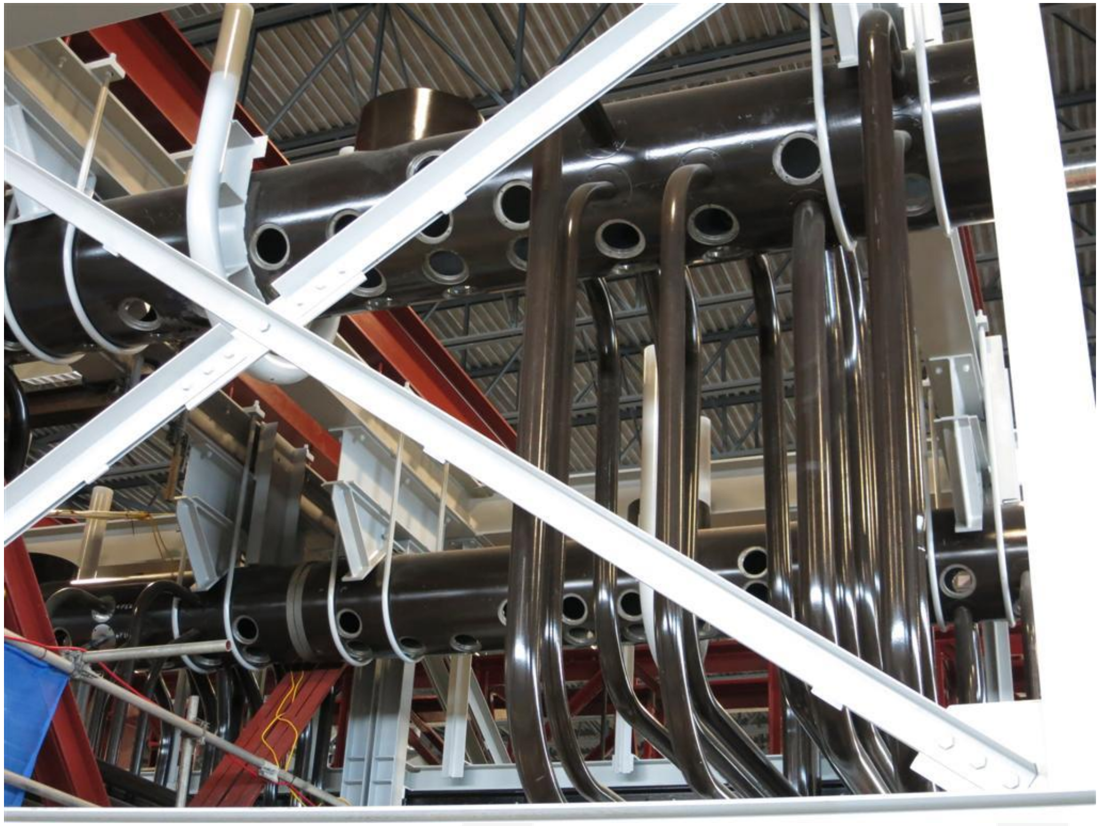
Feeder Tube Assembly

Feeder Piping in Mock-up Area

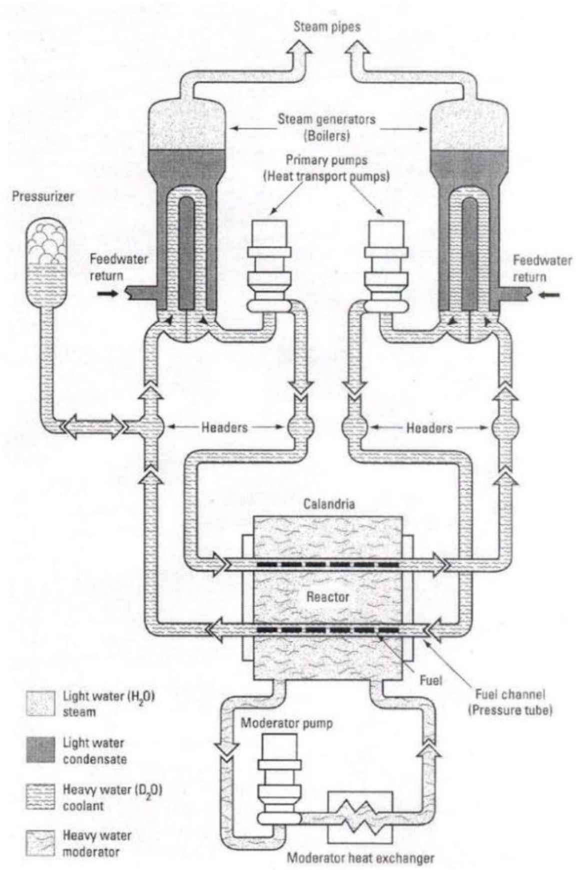
Reactor Face

Darlington

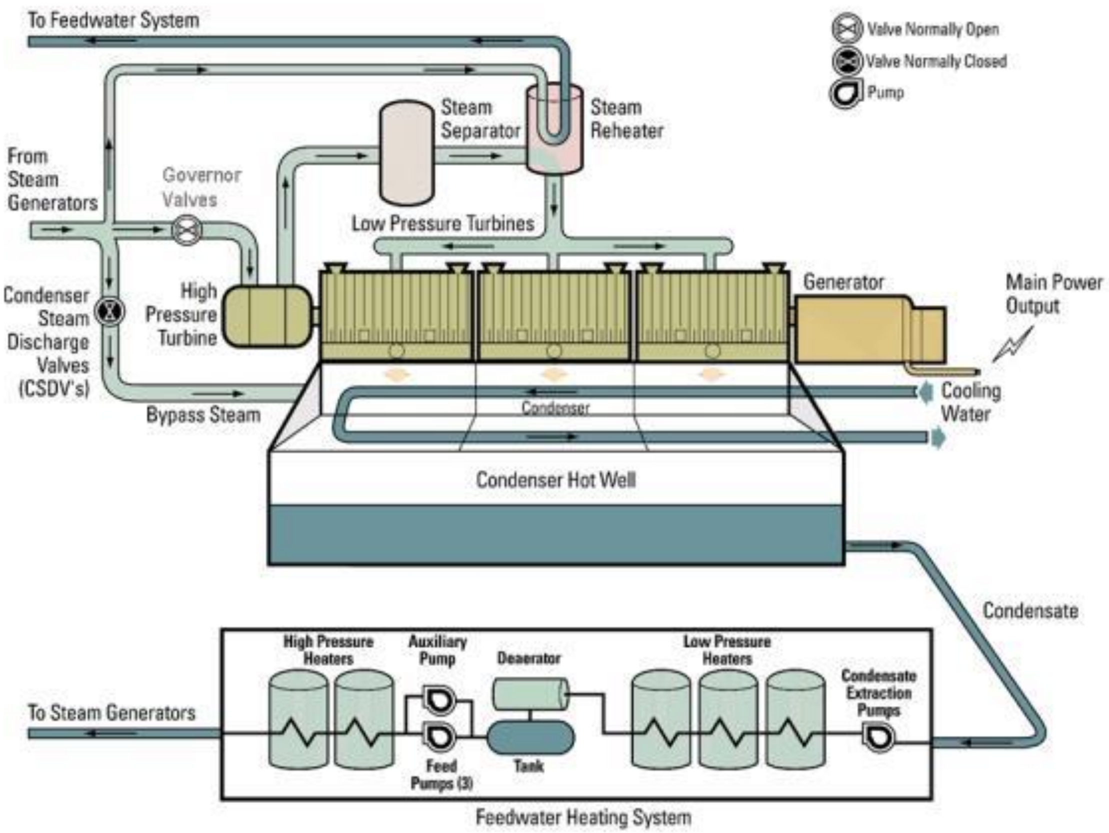
PHT Header and Feeders



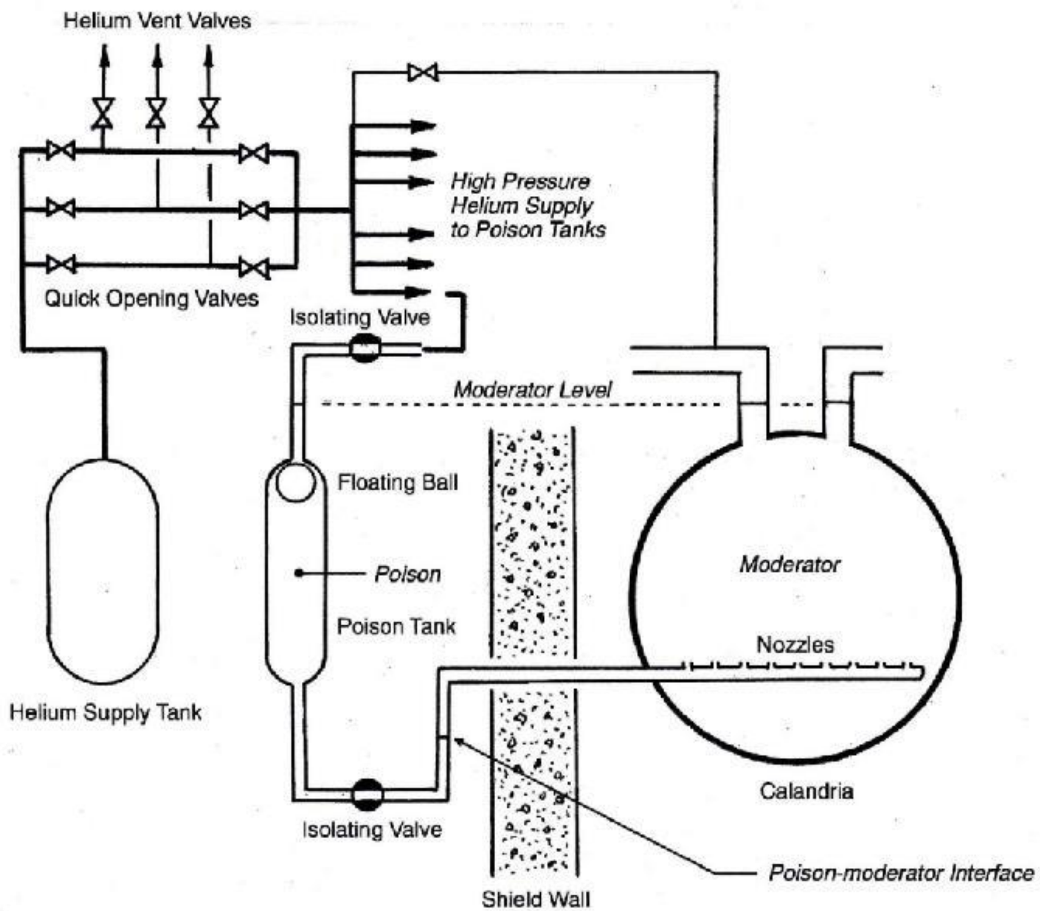
Moderator and Coolant Circuits



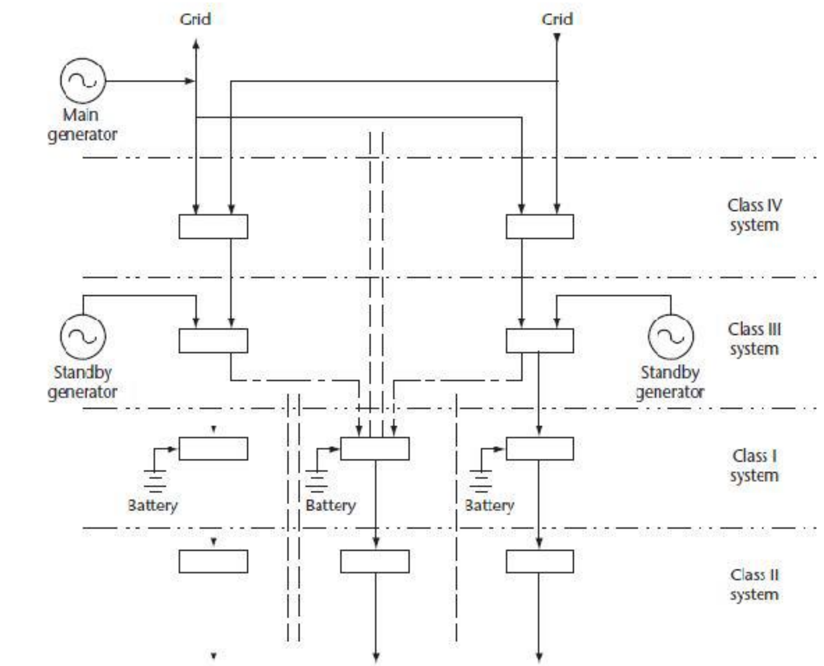
Turbine-Generator and Feedwater Systems



Shut Down System no 2



Electrical Distribution System



Legend:

- Buffered power source
- Class separation
- Distribution system and load group
- Division separation

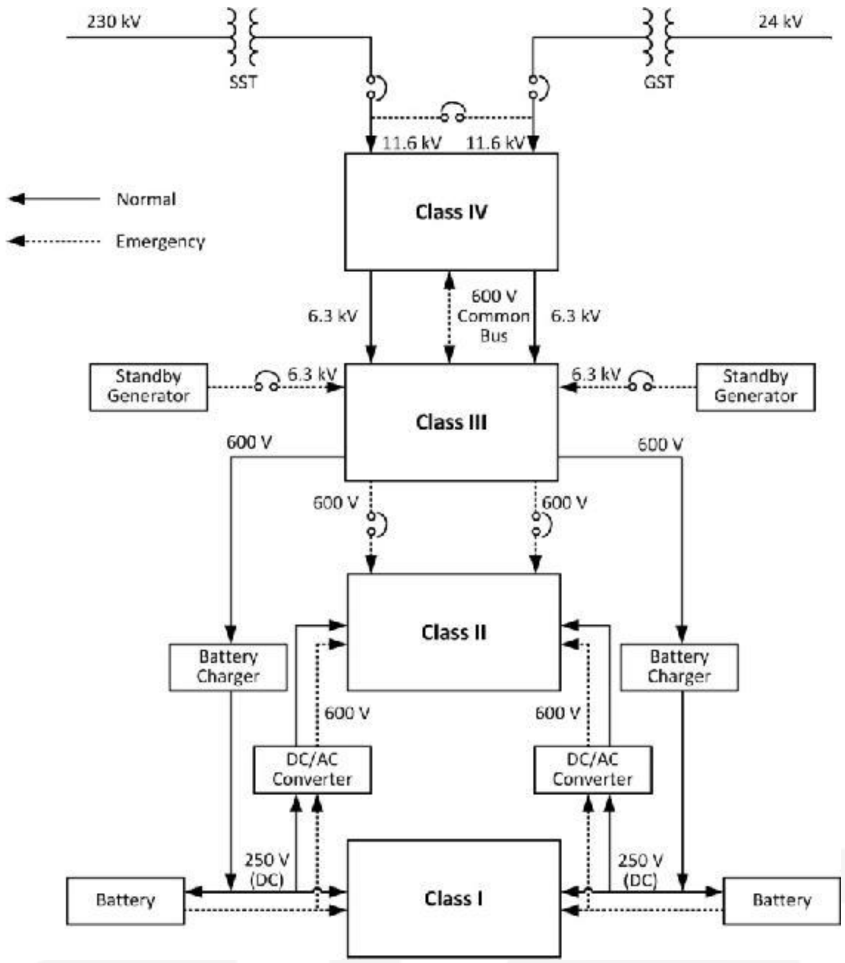
Notes:

(1) *This Figure provides a sample configuration; other configurations are possible.*

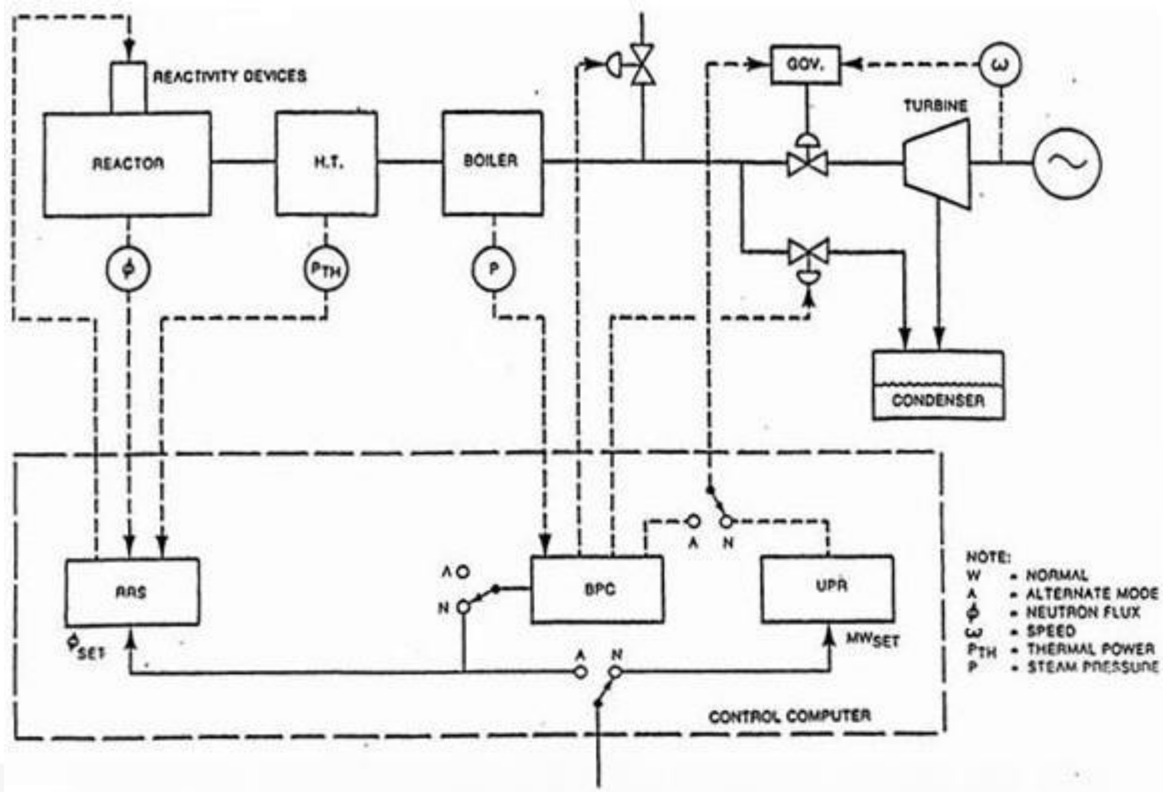
(2) *Not all required components are shown.*

(3) *Alternative power sources may be combined with the configuration in this Figure to meet the nuclear safety requirements of the plant.*

Classes of Power



Overall Plant Control



Main CANDU Control Programs

Program Name	Measured Parameter (s)	Variable(s) Controlled	Variable(s) Manipulated
1. Unit Power Regulator (UPR)	• Electrical output	• Electrical output	• Steam flow
2. Reactor Regulating System (RRS)	• Reactor neutron power • Reactor thermal power	• Neutron flux	• reactivity mechanisms - control rod position - zone water level
3. Heat Transport Pressure and Inventory Control (HTP&I)	• Reactor Outlet Header pressure	• Pressurizer pressure • Pressurizer level	• Pressurizer steam bleed & heaters • D_2O feed & bleed
4. Steam Generator Pressure Control (SGPC)	• Steam Generator pressure • Reactor power	• Steam Generator pressure	• Reactor setpoint • Steam flow
5. Steam Generator Level Control (BLC)	• Steam Generator level • Reactor power • Feedwater flow • Steam flow	• Steam Generator Level (inventory)	• Feedwater flow

Risk Concept

- All human activities pose a risk
- Risk = Probability X Consequences
- Minimizing the Risk
- Factors in the Perception of risk:
  - Voluntary or not
  - Emphasis on consequences
  - Understanding the Technology

- Personal choice, or Society

CANDU Principles

- Regrouping Systems by importance wrt a safety function:
  - Special Safety
  - Standby Support
  - Safety Related
  - Process Systems

- Operating Principles
  - 3Cs: control cool contain
  - Prescribed testing
  - Preventive Maintenance
  - Periodic Inspections Program

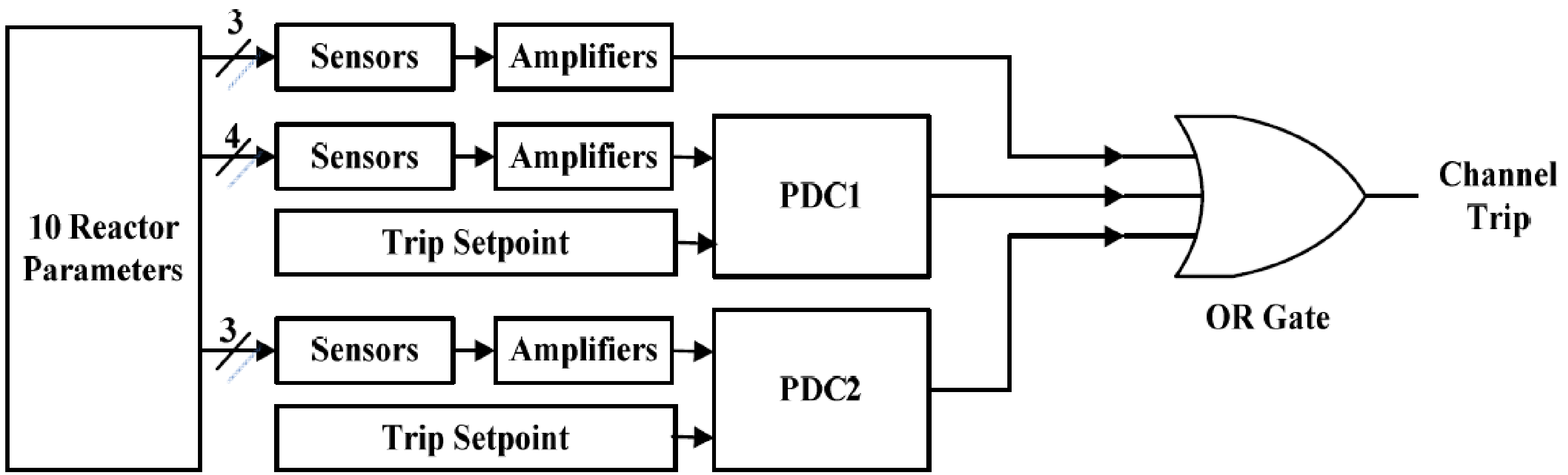
Design Principles

- Design to strict rules
- Defense in depth: Design, Maintenance Operation to a number of barriers (between you and harm): weakness of anyone of the multiple barriers still requires you to repair the weak barrier.
- Barriers are detectable for failure, repaired and tested.

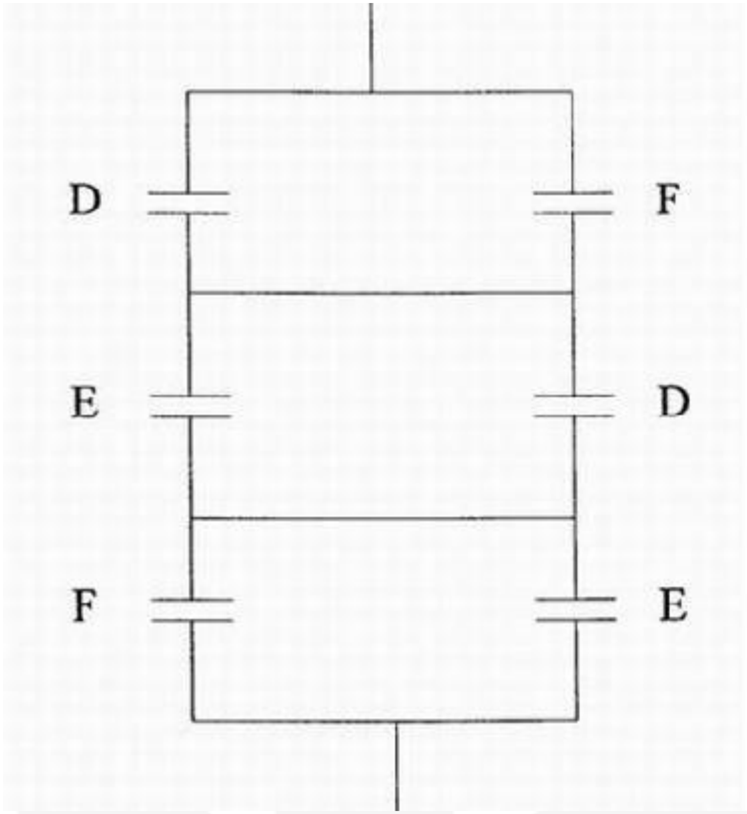
Design Principles

- Redundancy: 2 X 100 % pumping capacity;
- Independence: 2 different means of achieving redundancy, which are also not sharing common components (as mucha s possible);
- Diversity: 2 ways of achieving the same result; wearing belt and suspenders;
- Safe failure: when a component fails, it fails in a mode that provides the safest function for the overall safety; example; a fire door closes; a loss of brakes signal might engage the brakes;
- Triplication: 3 signals or parameters are measuring ONE parameter, independent; you may combine the signal, average, select high, low on failure of one; allow selection of faulty signal; reject a signal to test it .

Shut Down System no 1 Trip Channel

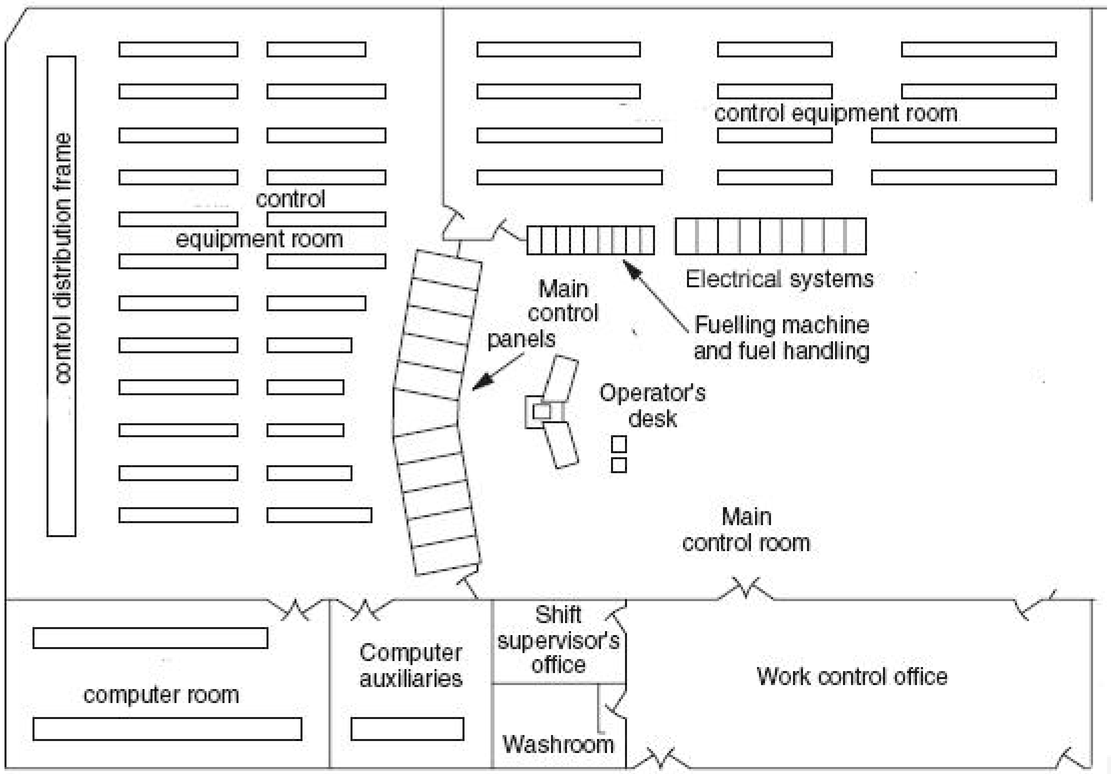


2 out of 3 Trip Logic

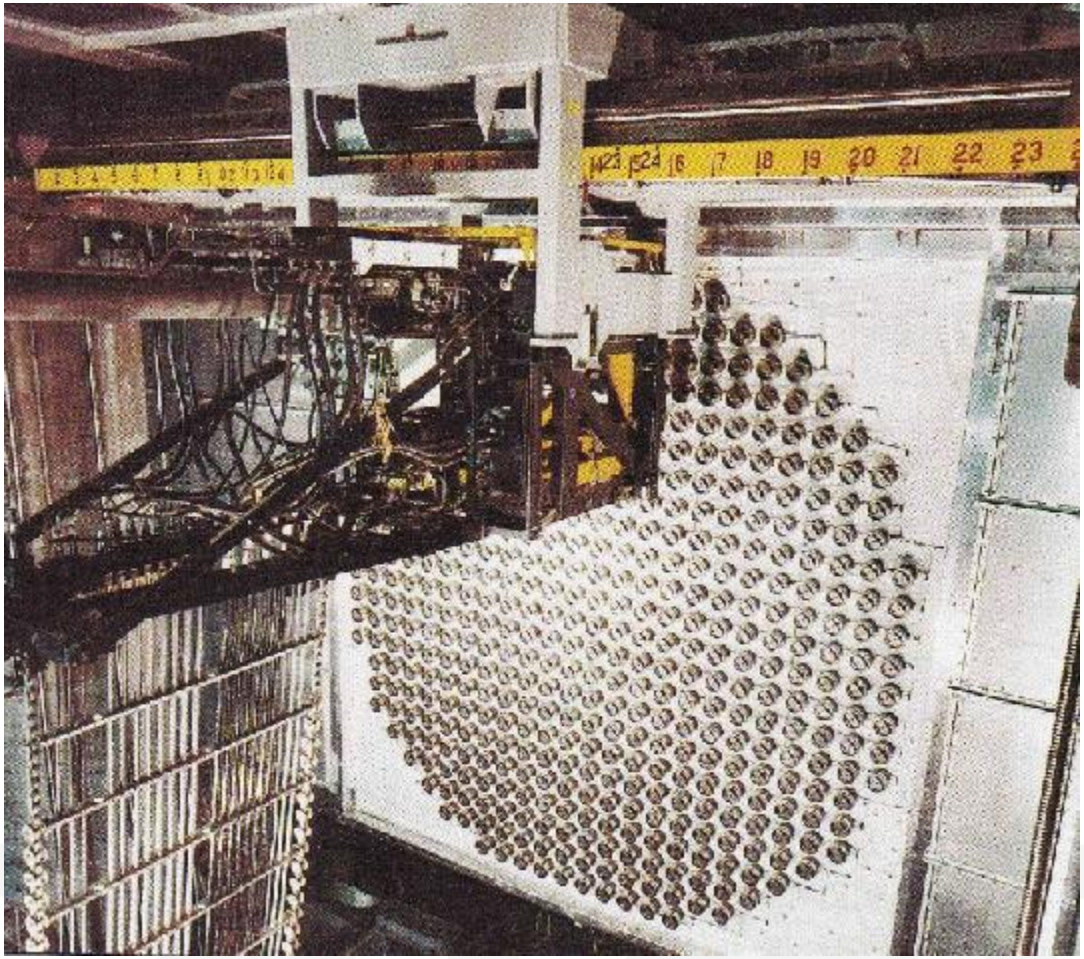


Control Room

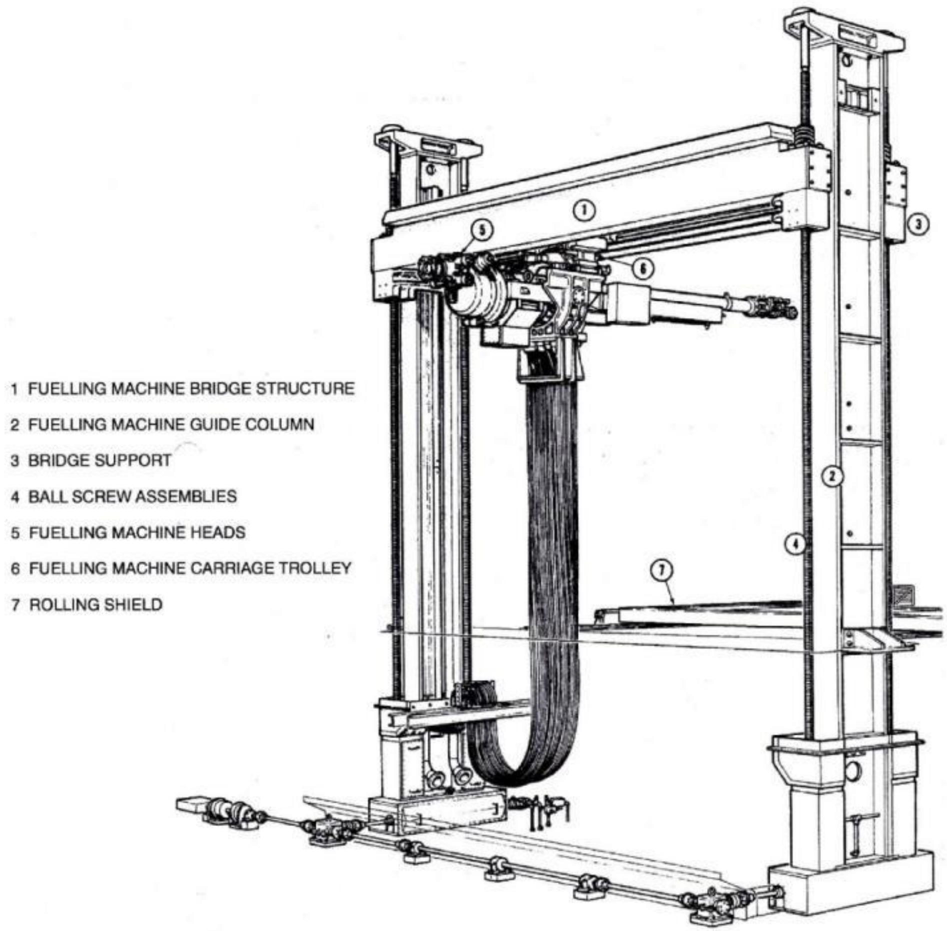
Control Room Schematic



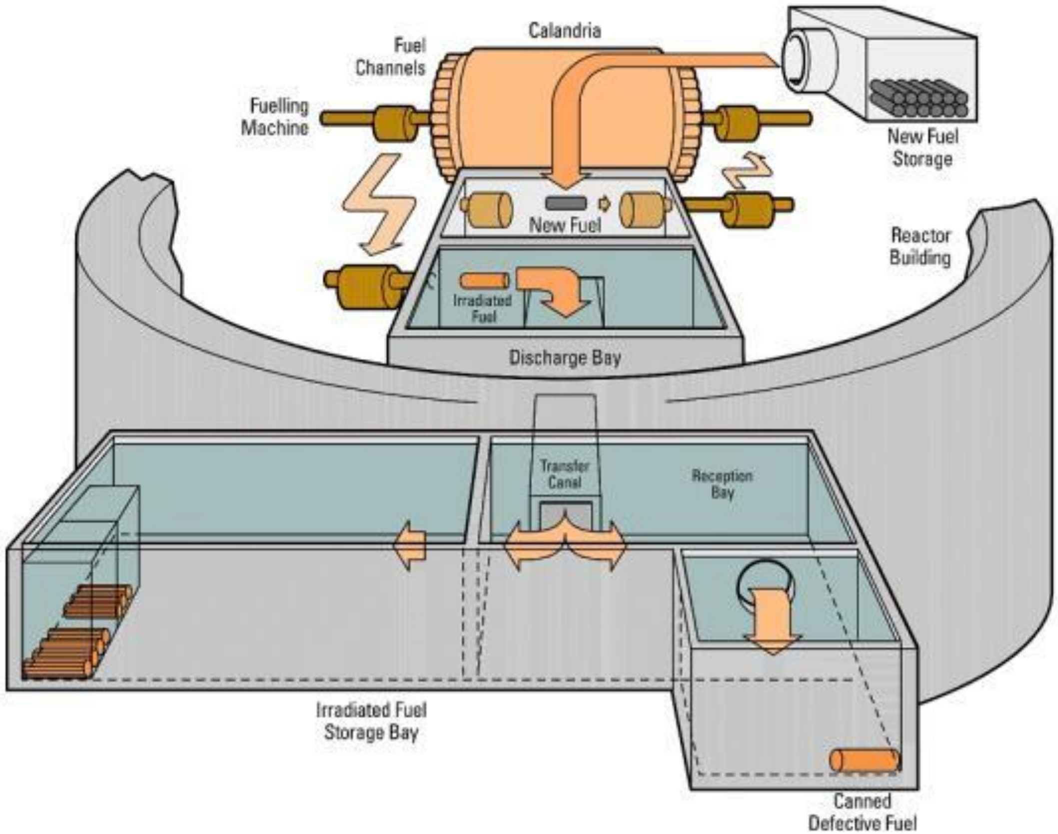
Reactor Face with Fuelling Machine



Fuelling Machine and Bridge



Spent Fuel Management



www.nwmo.ca

- Long terme; combustible irradié:
- Obligation d’étudier au moins trois solutions
- l’évacuation en couche géologique profonde
- le stockage sur les sites des réacteurs nucléaires
- le stockage centralisé – soit en surface, soit sous terre
- Gestion adaptative progressive: solution choisie
- dialogue maintenu pendant trois ans avec le public
- accent sur l'adaptabilité
- nouvelles connaissances ou changements dans les priorités de la société
- points de décision explicites ; participation du public
- décision d'aller de l'avant ou non à chaque étape

The Used Fuel

- Responsabilité des exploitants selon la loi
- Court terme
- Grappes entreposées dans des bassins d’eau
- Outils spéciaux de manipulation
- Moyen terme
- Grappes transférées dans des conteneurs de stockage à sec
- Silos ou modules en béton

Learning from Events

- Three Mile Island -2
- PWR (cuve pressurisée)
- Pennsylvanie, États-Unis
- Accident en 1979
- Perte de refroidissement causé par l'ouverture d'une vanne… (mal interprété)
- Niveau apparent - formation des opérateurs
- Fonte du cœur
- Peu de conséquences en rejets dans l'atmosphère
- Gestion de crise

Learned

- TMI-2 :

- La formation des opérateurs
- La gestion des salles de commande
- L'injection d'eau haute pression au coeur

Learning from Events

- Challenger :
- Navette spatiale, Floride, États-Unis
- Explosion au-dessus de l'Atlantique en 1986
- Risques connus
- Risques ignorés
- Pressions de la gestion (coûts)
- Culture de l'entreprise

Learned

- Challenger:

- La culture de sûreté
- Les plans d’urgence

Learning from Events

- Tchernobyl-4 :
- RBMK, Ukraine, URSS
- Explosion en 1986
- Mauvaise conception (contrôle normal trop lent)
- Mauvaise conception (cuve trop large)
- Mauvaise conception (graphite)
- Mauvaise conception (arrêt, confinement)
- Non-respect des règles (6 en série)
- Mauvaise écoute de l’agence de réglementation

- Tchernobyl-4:

- La robustesse de la conception – le confinement
- La formation du personnel
- L’utilisation des études probabilistes

Learning from Events

- Davis-Besse :
- PWR, Oak Harbor, Ohio, États-Unis
- Accident évité de justesse en 2002
- État lamentable de la cuve du réacteur – risque de bris catastrophique à haute pression
- Les indications étaient disponibles
- Mauvaise gestion du titulaire

Learned:

- Davis-Besse:
- L’inspection des systèmes de gestion

Learning from Events

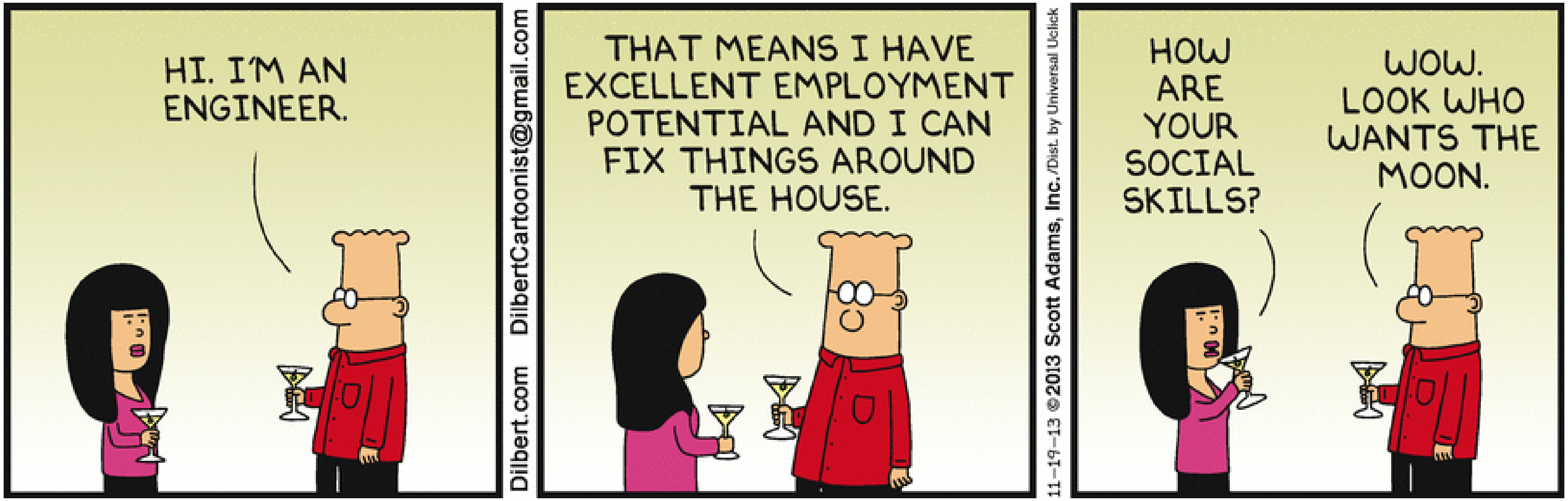
- Fukushima :
- BWR, Fukushima, Japon
- Accident en mars 2011
- Survécu au tremblement de terre
- Problème d’inondation
- Mauvaise conception (mur anti-tsunami)
- Mauvaise conception (localisation, dimension et capacité des piscines)
- Mauvaise préparation aux incidents hors-dimensionnement
- Mauvaise gestion des connaissances
- Les détonations d’H2

Learned

- Fukushima:

- Prévoir l'imprévisible – le gérer
- Les plans d'urgence
- La robustesse

Being an Engineer…



Discussion

Comparaisons (selon DOE (US) et CCSN):

- Personnel typique	3-4 mSv/an
- Limite pour les travailleurs:	50 mSv/an - 100 mSv/5 ans (?)
- Limite pour le public:	1 mSv/an
- À 1 km d'une centrale:	0.02 mSv/an
- Pilote d'avion commercial:	3 mSv/an
- Sources naturelles moyenne USA:	3 mSv/an
- Sources naturelles Yangjiang Chine:	6 mSv/an
- Retombées des essais de bombes	0.02 mSv/an
- Produits de consommation	0.02 mSv/an
- Rayon X dentaire	0.1 mSv
- CT scan	10 mSv
- Baryum GI	85 mSv
- Voyage Londres NY	0.1 mSv
- Mission ISS:	100 mSv
- Dose mortelle 50% (aigu)	4.5 Sv sans traitement
- Légère hausse notée cancers	100 mSv aigu
- ou chronique	200 mSv

nuclearsafety.gc.ca

facebook.com/CanadianNuclearSafetyCommission

youtube.ca/cnscccsn

Canada