UNIVERSITY OF CAMBRIDGE

Regulating the ways of making nuclear safe

Hong Kong Nuclear Society Seminar on Nuclear Safety – 8 Jan 2013

Tony Roulstone

January 2013

Nuclear Renaissance

Drivers for investment in nuclear:

- Energy security
- Climate change

Nuclear generation and plans for new nuclear:

Current reactors	435	377GWe	13.5%
Under construction	78	~70GWe	
Planned	160	177GWe	
Proposed	320		

- Largest programmes: China, S Korea & India
- Significant plans: US & UK
- Strong interest in E Europe
- New entrants: UAE, Vietnam, Turkey, Jordan, Bangladesh, Saudi Arabia, S Africa.

Safety questions?

- How can we ensure technically that nuclear is safe?
- What are the ways of regulating to make nuclear safe?

Nuclear Safety Scares

- Images of Fukushima (2011) and Chernobyl (1986) – feed the worst fears of the public – link to earlier images of nuclear bombs and the pervasive fear of radiation;
- Are such event inevitable?
- How can nuclear be made safe – and be seen to be safe?

Learning the Lessons

1. Major accidents/incidents are drivers of innovation in safety;

2. Look at Fukushima and Chernobyl as illustrating the principles of safety;

3. Also, consider two earlier accidents in UK and US -> drivers of two somewhat different safety approaches;

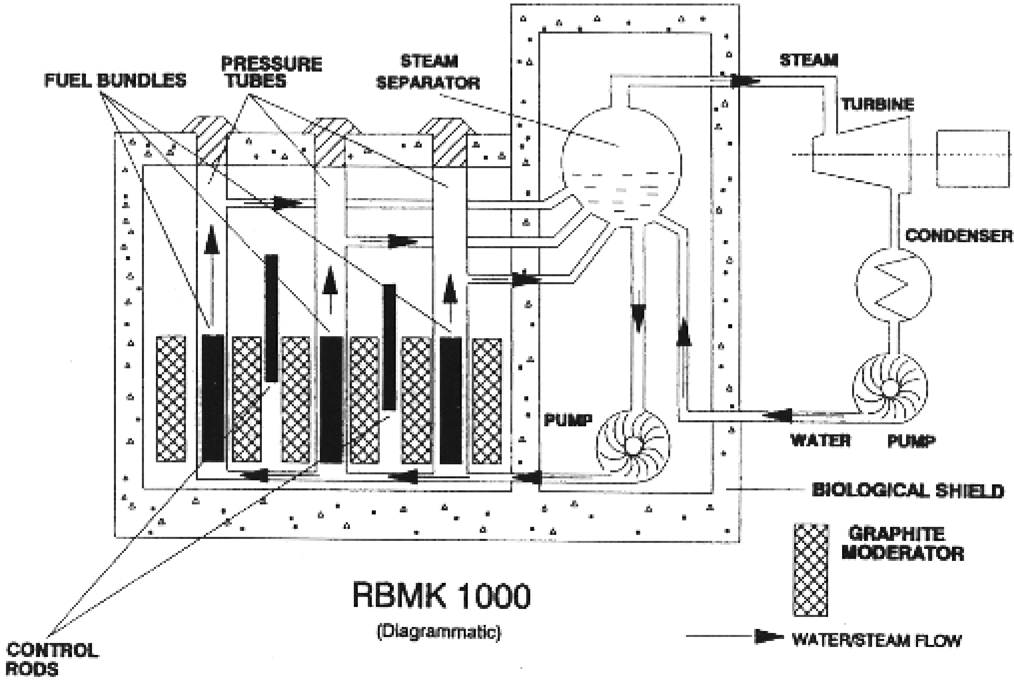
4. Review modern nuclear safety ideas;

5. In the context of the global nature of nuclear:
   - What is good practice?
   - What are the structures of regulation that work?
   - What needs to be improved?

Chernobyl - Loss of Power Control (1)

- Chernobyl RBMK design – boiling water cooled graphite moderated reactor;
- Accident occurred during a test to look at cooling after a trip of the reactor
- The ECCS was isolated using the manually operated valves.
- Test was started from 200MWt and with the reactivity margins of the manual control rods were severely
- Turbine switched off to simulate a loss of unit power - reactor scrammed and a large reactivity excursion;
- Power surge >140 times maximum.

-> plant explosion

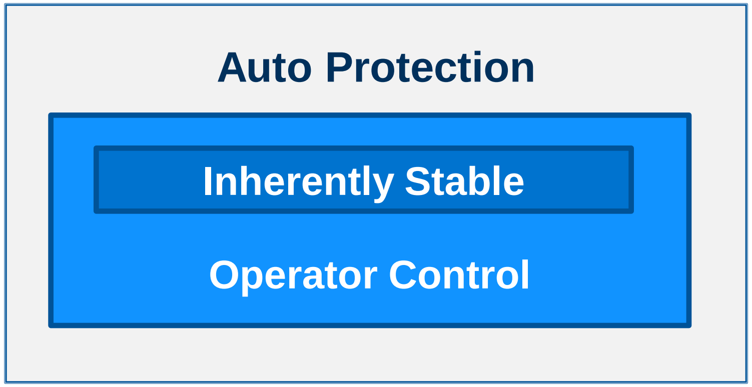


Chernobyl - Loss of Power Control (2)

- Power control was lost – because of **inherent** design weaknesses:
  - Positive ‘void coefficient’ – boiling in the core as cooling pumps ran down, increased reactivity & hence power – viscous circle;
  - Insertion of control rods initially added reactivity – worsening effect;
- Accident had **larger effects** because of other design features:
  - Escape of steam reacted with graphite moderator creating hydrogen & a later fire;
  - Ineffective containment – contain radioactivity & mitigate wider effects.
- Widespread effects due to:
  - Energy of reaction dispersed radioactivity widely;
  - Slow reaction to emergency – local public health.

Principles of power control

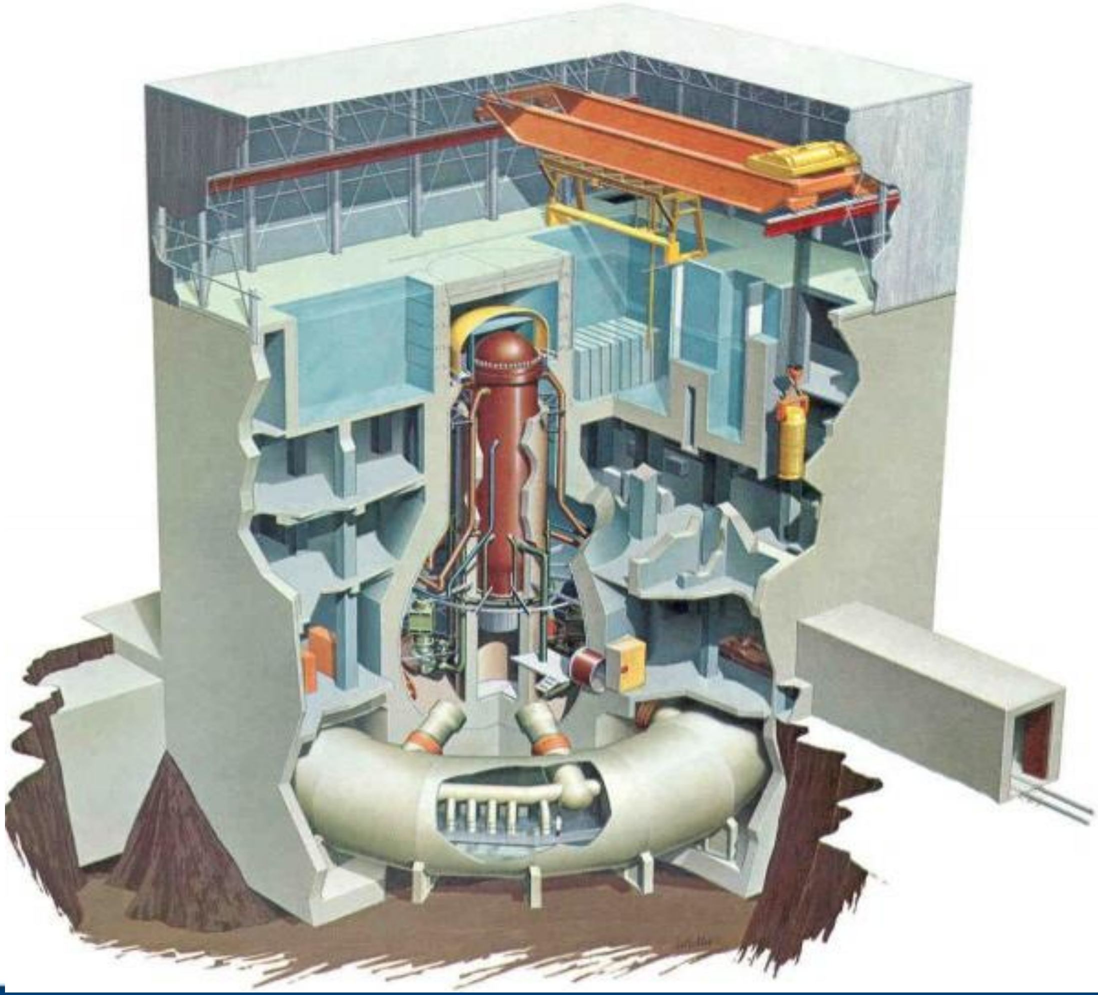
Three levels of control & protection – Defence in depth;



1. Inherent reactivity stability – by design,
2. Operator control of reactivity – understand and reduce reactivity,
3. Safety protection – automatic and unequivocal shutdown.

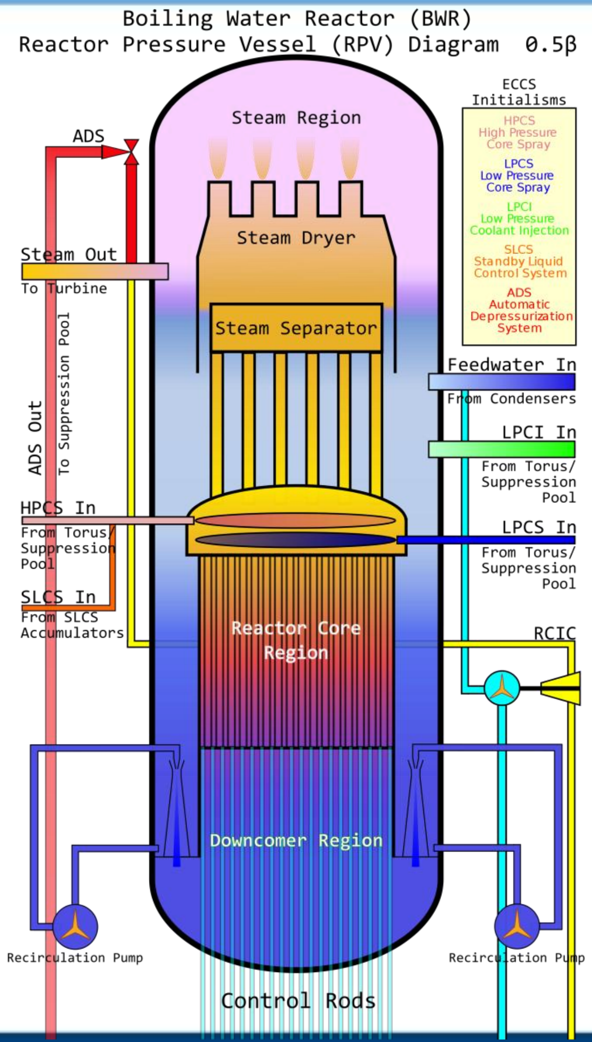
Fukushima - Loss of Cooling

- Fukushima – early version of a Boiling Water Reactor:
- Second most popular type in the world ~120 built;
- Single reactor vessel surrounded by low pressure steam containment vessel – with a cooling toroid;
- Building and shielding protects workforce;
- Weak containment design allowed hydrogen and radioactivity to be released.



Fukushima – Loss of Cooling

- Single reactor vessel:
  - Water circulated over fuel rods;
  - Heat removed by boiling;
  - Steam separated above core.
- After earthquake reactor shutdown and cooling established;
- Tsunami – destroyed off-site power lines, flooded diesel generators and switchboards;
- Station blackout meant no water to vessel which was quickly emptied by effect of decay heat from fission products;
- Decay heat melted fuel clad which reacted wit water to make hydrogen which exploded on contact with air.



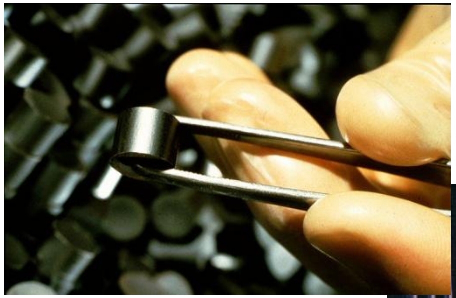
Principles of Cooling & Containment

Barrier 1 - Fuel Clad

Barrier 2 - Reactor Vessel

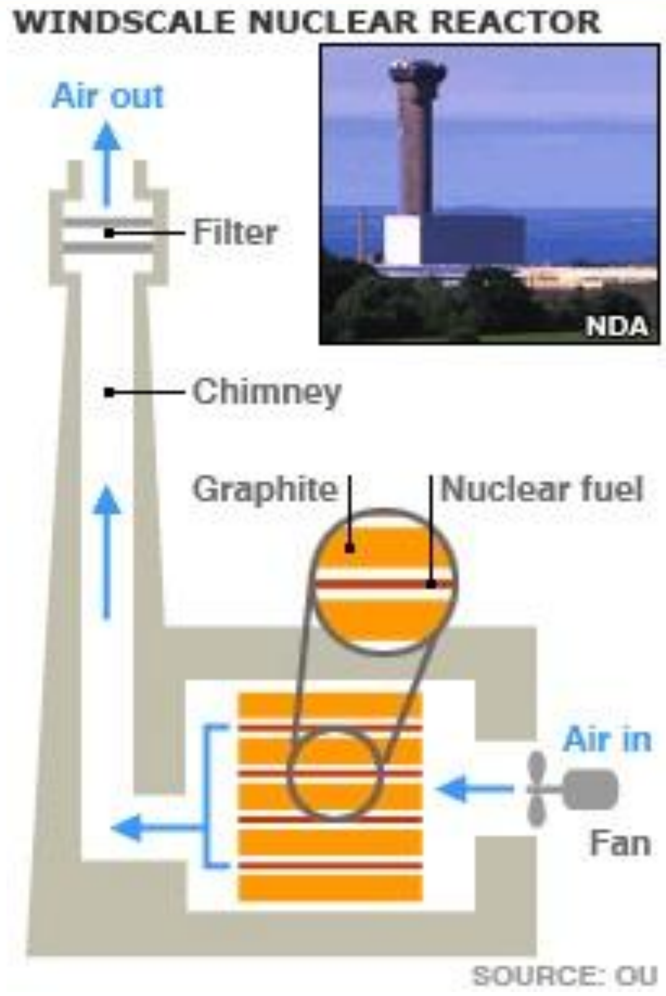
Barrier 3 Effective Containment

- Defence in depth:
  - Reliable cooling systems;
  - Diverse and secure power sources;
  - Effective containment design



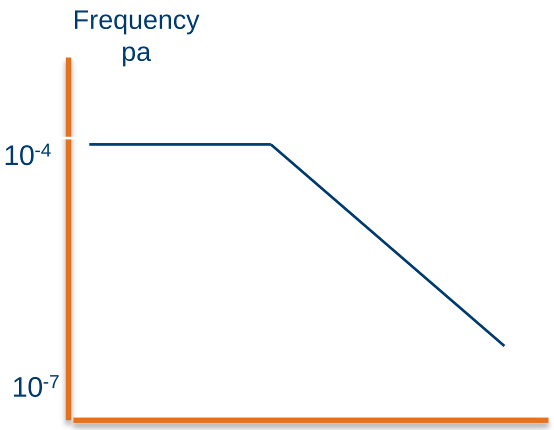
UK and Windscale (1957)

- Air-cooled weapons reactor caught fire due to build-up of energy in the graphite matrix from the effect of neutrons;
- Release of energy in the graphite moderator led to both the graphite and the fuel catching fire;
- Radioactivity released from the burning fuel blown up the chimney and spread by the wind across the UK;
- Some protection provided by:
  - Chimney filter;
  - Distribution of iodine tablets and
  - Food monitoring & disposal.



Effect on UK Nuclear Regulation

- **Trust** in ability of scientists/engineers to self- regulate **was** broken:
  - Establishment of independent nuclear safety teams – as NII/ONR inspectors;
  - NII/ONR separate in function and control from energy investment & promotion – able to shut down operations;
  - Process of application for safety authorisation before build, periodic re-authorisation throughout life and site inspection.
- Emerging body of knowledge & the variety of designs:
  - **Principles-based** safety case rather than fixed criteria
  - **Owner/operator** makes and maintains the safety case;
  - Beginnings of **risk-based** views of safety.
- Recognise the importance of off-site, public health safety.



Public Safety Target

Three Mile Island – 2 (1979)

- Pressurised Water Reactor – high power density in core;
- Most popular type of reactor >200 built – basis of most current new nuclear programmes;
- Minor coolant leak from a relief valve was not diagnosed by the operators;
- Misdiagnose led to wrong actions – pumps and water injection;
- Led to core being uncovered and major damage – which was contained – little off-site release of radioactivity.

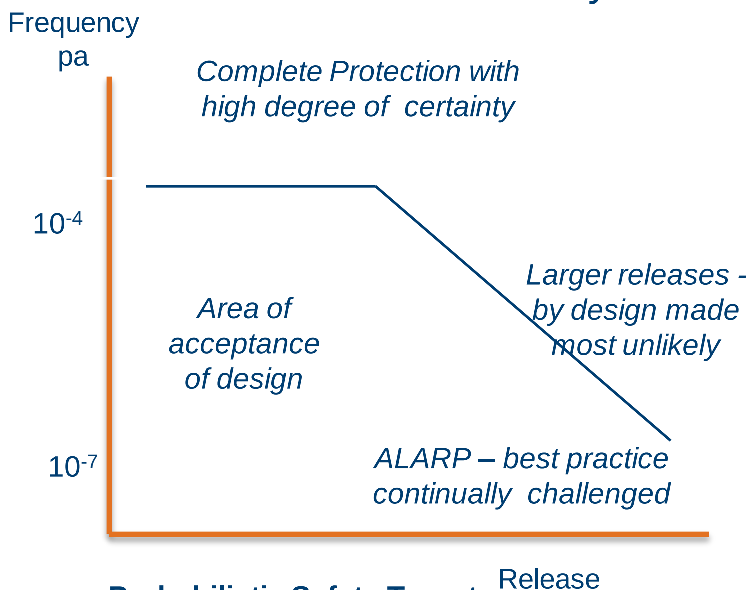
Effect on US Safety Regulation

- US nuclear regulation had been separated from energy promotion in 1974, creation of NRC – a legal body which sets the standards and approves licences;
- Legal/economic structures support NRC as setter of standards – ‘rule making’ – which enforces common approach but takes some responsibility from operators;
- Before TMI safety case was somewhat simple:
  - Protect single fault plus single subsequent failure criterion;
  - Containment to mitigate the effects of larger accidents
- Based on a lengthy ‘Lesson learned’ process involving many different groups and people from different countries:
  - Probabilistic methods came to the fore;
  - Human factors and control design important;
  - LOCA analysis and protection extensively studied and included in designs;
  - Probabilistic studies highlighted external hazards: earthquake, fire, flood etc.

Origin of Gen III+ reactor designs

Probabilistic Safety Methods

- Broad and comprehensive view of safety through probabilistic methods:
  - Failure Modes & Effects Analysis — FMEA
  - Event Tree Analysis — ETA
  - Fault Tree Analysis — FTA
  - Probabilistic Risk Analysis — PRA



Probabilistic Safety Target

Probabilistic Risk Analysis:

- Combines together **many possible accident** sequences
- Considers:
  - **Probability** or frequency of accident sequence
  - **Size** of effect/release
- Compares results with an explicit **safety target**

Safety Regulation has improved standards

- **Safety standards have risen** have improved during the 50 years of power reactors –
  - from design base accidents to probabilistic methods and
  - much wider range of hazards considered including internal & external hazards – fire, earthquake, flood, aircraft crash, terrorism etc.

- **The key issues for nuclear safety are**:

Core Damage Probability		**+**	**Effective Containment**
once in	1,000 reactor years		1970 BWRs & PWRs - as built
	10,000 reactor years		1970 reactors - upgraded after TMI
	100,000 reactor years		1980/90 reactors - such as UK, Sizewell B
	1,000,000 reactor years		Gen III+ designs such as EPR & AP1000

Achieving the highest standards of nuclear safety

- **Technical** means exist to make reactor accidents very remote and to mitigate the effects of any release;
- This low risk environment highlights the residual issues:
  - **Highly infrequent external events** – earthquake, wind, fire, flood, explosion, aircraft crash etc.
  - **Operational failures** – lack of knowledge/understanding, confusion under the pressure of events, poor communication;
  - **Safety regulation** – lack of tension between investors/operators and safety authorities.

Achieving the highest standards of nuclear safety

- **Highly infrequent external events** – earthquake, wind, fire, flood, explosion, aircraft crash etc.
- **Fukushima** – an example of external event considered beyond design basis & and therefore excluded from consideration;
    - Response:
        1. Robust reactor design that include a broad range of external event in design – Gen III+ reactors;
        2. Include very unlikely events in the safety case:
            - ASME Presidential Task Force – recommend consideration of ‘beyond design basis event’ for ‘cliff edge’ effects;
            - ALARP process as in UK.

Achieving the highest standards of nuclear safety

- **Operational failures**– lack of knowledge/understanding, confusion under the pressure of events, poor communication;
- **Chernobyl** – an example of operator triggered event (together with poor technical design);
  - Response:
    1. Safety as the day-to-day ‘mantra’ of nuclear operators – their highest goal;
    2. Spread best practice in operations – WANO independent peer reviews – process needs strengthening after Fukushima where weak maintenance practices seem not have be identified.

Achieving the highest standards of nuclear safety

- **Safety regulation** – lack of tension between investors/operators and safety authorities.
- In many countries including Japan – lack of clarity between the promoters and the regulators of nuclear energy;
  - Response required:
    1. Regulation on a statutory basis;
    2. Separation and tension between & operators
    3. Stronger international standards.

Fukushima – Diet Commission Exec Summary

- What must be admitted – very painfully – is that this was a disaster "**Made in Japan**."
- Only by grasping this mindset can one understand how Japan's nuclear industry managed to **avoid absorbing the critical lessons learned** from Three Mile Island and Chernobyl; and how it became **accepted practice to resist regulatory** pressure and cover up small-scale accidents.
- It was this **mindset** that led to the disaster at the Fukushima Daiichi Nuclear Plant

Best Practice in Safety & Regulation

Design safety

- Design base accidents protected/precluded;
- All risks are examined and reduced
  – more effort on the more frequent events

Organisation

- Nuclear utility is responsible for making and maintaining a safe plant;
- Whole life concept of safety – initial, site inspection plus periodic reviews;
- Capable/responsible operating organisation/staff.

Regulation

- Independent & effective nuclear regulator;
- Good emergency planning – practiced/resourced.

Opportunities for improvement

- Common and enforceable safety rules for a global industry which has global effects;
- Extending the range/frequency of events considered/protected e.g. tsunami-like.

Tony Roulstone

armr2@cam.ac.uk

Department of Engineering
University of Cambridge
Trumpington Street
Cambridge CB2 1PZ

+44 775 362 7634