BASIC CONCEPTS OF NUCLEAR SAFETY

IAEA Workshop on Severe Accident Management Guidelines

15–16 December 2016, Vienna, Austria

presented by

Randall Gauntt (SNL)

IAEA

International Atomic Energy Agency

IAEA
International Atomic Energy Agency

Outline

- Introduction to nuclear safety
  - Basic facts
  - Fundamental safety principles
  - Defence-in-depth
  - Safety functions
  - Initiating events
- Plant features and behaviour
  - Basic elements
  - Structures, symbols and components
  - Accident scenario classifications
  - Acceptance criteria
  - Plant operation and configuration
  - Instrumentation and control

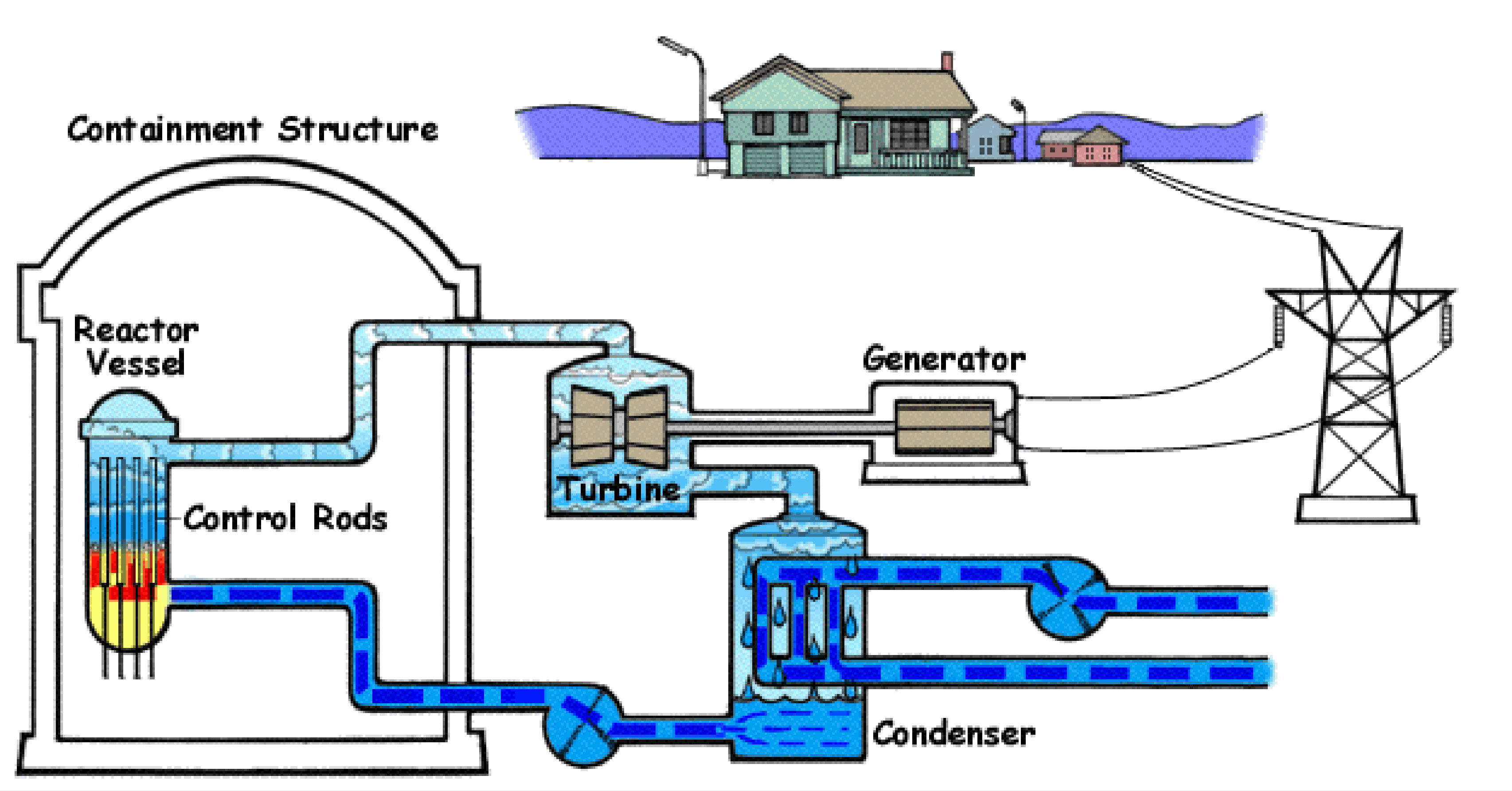
Basic facts

The course considers light water reactors (LWRs) and pressurised heavy water reactors (PHWRs);

These can be *direct cycle* (steam is generated in the core and directly transported to the turbines, e.g. boiling water reactors (BWRs) or *indirect cycle*, where heat from the core goes to a steam generator, from which steam goes to the turbine, e.g. pressurised water reactors (PWRs), also PHWRs;

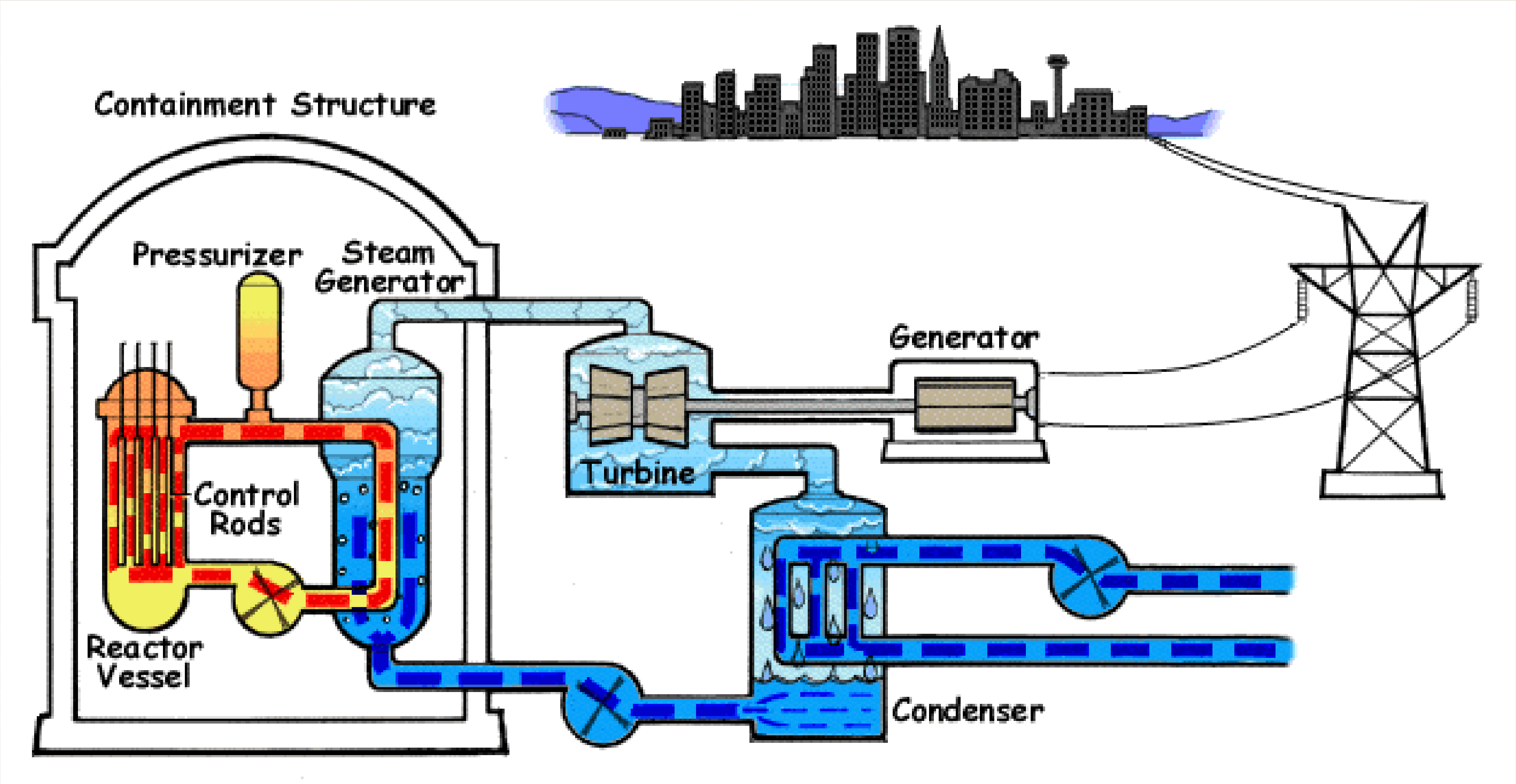
This presentation covers fundamental safety principles applicable to all types, followed by a summary of plant features and behaviour.

Schematic of a Boiling Water Reactor



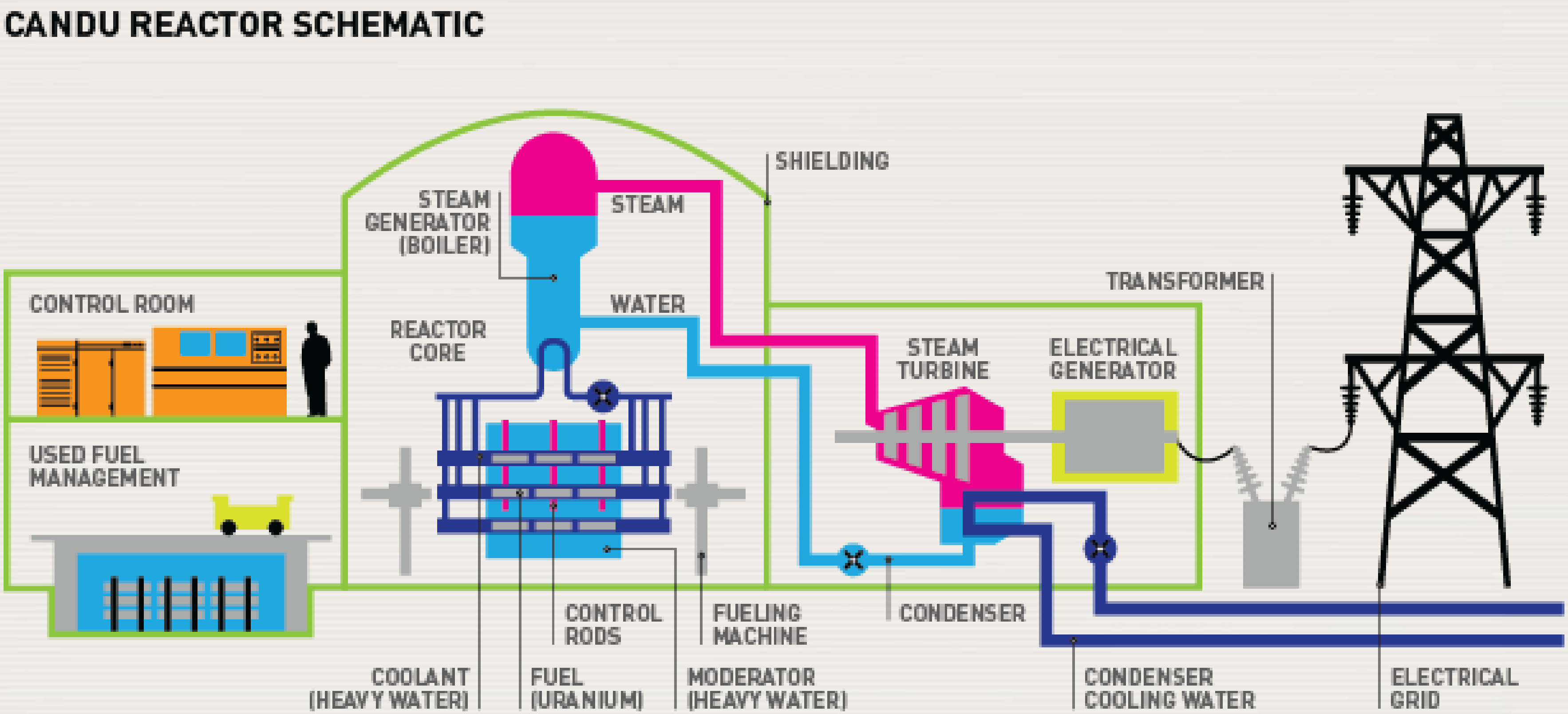
[www.usnrc.gov]

Schematic of a Pressurised Water Reactor



[www.usnrc.gov]

Schematic of a Pressurised Heavy Water Reactor



[www.cna.ca]

Fundamental Safety Objective

To protect people and the environment from harmful effects of ionising radiation;

To achieve this objective, nuclear power plants are designed and operated so as to achieve the highest standards of safety that can reasonably be achieved. This includes:

- **Control of radiation exposure;**
- **Control release of radioactive material to the environments;**
- **Restrict the likelihood of an accident with inadvertent release of radionuclides;**
- **Mitigate the consequences of such an accident;**

Important elements of nuclear safety are the principle of defence in depth and the definition and application of safety functions.

Defence in depth

Defence in depth is a concept of independent and subsequent layers of safety measures;

- **Failure of one level is mitigated by features in the next layer;**
- **In nuclear power plant safety, multiple and successive physical barriers are provided against the escape of fission products to the environment;**
- **This is achieved through different levels of protection, which are detailed below;**
- **This concept is also used widely outside the nuclear sector, where the number of levels depends on the application.**

Levels of protection (1/3)

Five levels are defined:

- **The *first level* deals with high quality of the reactor circuit, so that the probability of accidents is low;**
- **The *second level* should prevent deviations from normal operation to develop into accidents, by specific systems, design features and operating procedures. Such deviations may occur once or several times during plant life. Supporting procedures are Abnormal Operating Procedures (AOP), or similar other names;**
- **The *third level* assumes that despite the provisions in the first and second level, accidents may occur, up to and including the design basis accidents/events (DBA, DBE);**
  - Mitigation is done by dedicated engineered safety features, safety systems and the associated procedures, the Emergency Operating Procedures (EOPs). DBA / DBE are not expected to occur, but are postulated to determine the design basis of the plant;

Levels of protection (2/3)

Five levels (continued):

- The *fourth level* provides protection for highly improbable accidents, the 'design extension conditions' (DEC), notably through maintaining the containment function. Supportive procedures are the Severe Accident Management Guidelines (SAMG);
- Should the 4th level fail, notably the containment, then emergency measures are taken in the environment, to protect the people and the environment, which is the *fifth level*.

Levels of protection (3/3)

Event Frequency	DiD Level	Plant Condition	Objective	Means	Radiological Consequences
Expected During Lifetime of Plant	Level 1	Normal Operation	Prevent Failure & Abnormal Operation	Conservative Design/High Quality Construction	Operation Discharge Limits
	Level 2	Operational Occurences	Control Failures & Abnormal Operation	Control, Limiting and Protection Systems, Surveillance	Operation Discharge Limits
Rare & Unlikely Events	Level 3a	Single Initiating Event	Accident Control Prevent Core Damage/ Core Melt Limit Release	Safety Systems Accident Procedures	Minor Off-site Radiological Impact
	Level 3b	Selected Multiple IE		Safety Features Accident Procedures	
Extremely Rare Events	Level 4	Core Melt Accident	Elimination of Large or Early Release	Safety Features for Mitigation	Protective Measure (limited in area & time)
Emergency Planning	Level 5	Significant Release	Mitigation of Radiological Impact	Off-site Emergency Response	Drastic Protective Measures

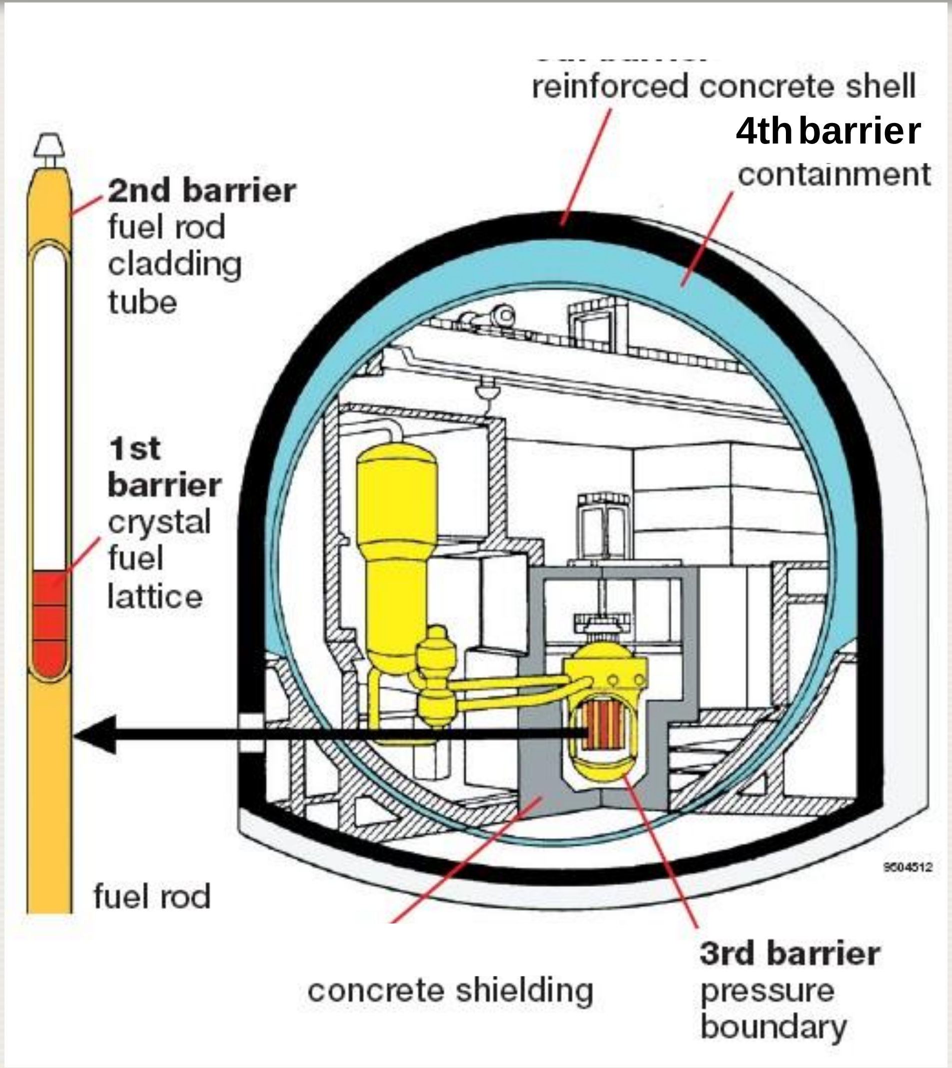
Barrier concept of Defense in Depth

Multiple technical and physical barriers between the fission products in the reactor core and the environment:

- **Fuel matrix;**
- **Fuel cladding;**
- **Primary system pressure retaining boundary of the reactor coolant;**
- **Containment;**

Barriers are supported by additional retaining functions like water layers, pressure differences, filters in ventilation systems.

Physical Barriers



Dedicated systems are in place to protect the integrity of each of these barriers

Safety Functions

Three fundamental safety functions must be assured:

- **Control of reactivity;**
- **Removal of heat from the fuel rods;**
- **Confinement of radioactive materials and mitigation of releases;**

A nuclear power plant has structures, systems and components (SSC) that separately or together perform these functions;

Equipment is classified into items important for safety (safety systems) and those that are not;

- **Safety systems ensure the safe shutdown of the core, the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents.**

Safety Function: Control of reactivity

Control and limit reactivity changes:

- Reactor core;
- Fuel storage;

Guarantee safe shutdown:

- Prevent damage to fuel elements;
- Keep thermal power in safe range;

Important features:

- Inherently safe behaviour of reactor core;
- Effective and reliable control rods and SCRAM function;
- Secondary shutdown, esp. by boron injection for LWR.

Safety Function: Cooling of Fuel

Maintain coolant (water) at the fuel elements;

Reliable heat sinks for (residual) thermal power in:

- **Reactor core:**
- **Fuel storage:**

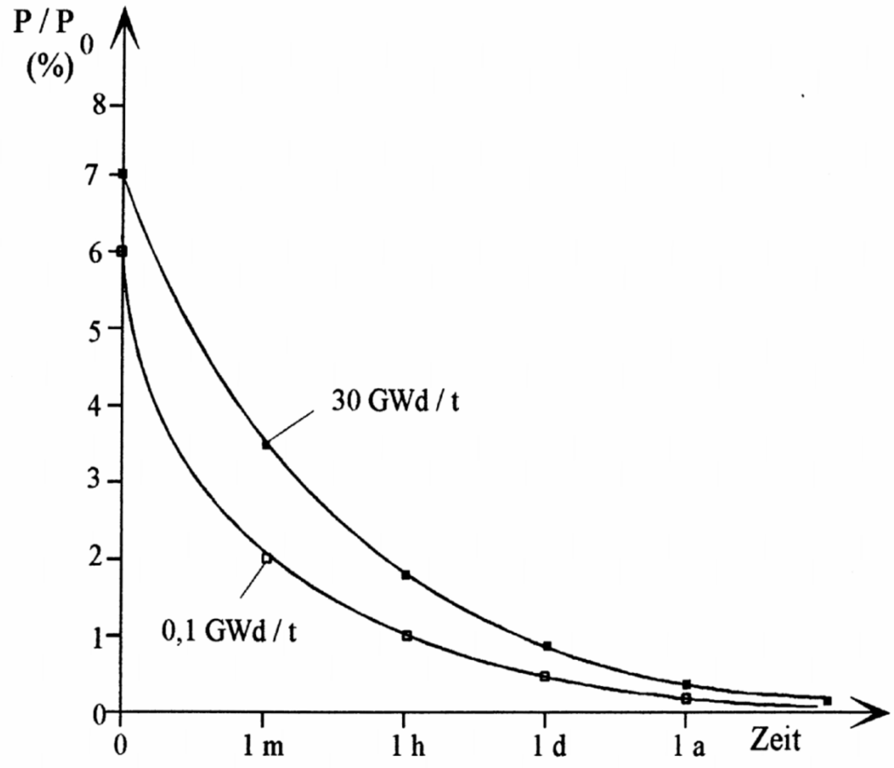
Reliable heat transport:

- **No Departure from Nucleate Boiling (DNB)**

Important features:

- **Main heat sink (condenser) and auxiliary heat sink (release valves);**
- **Integrity of primary coolant pressure boundary;**
- **Active recirculation and/or natural convection;**
- **Safety injection and heat removal systems.**

Residual Power



Trend of residual power with two different burn-ups

Safety Function: Confinement of Radioactivity

Safely close-off potential release paths;

- Degradation mechanism: corrosion, stress loads, irradiation, wear & tear, etc.

Shielding of direct radiation;

No impairment of heat removal;

Implementation;

- Designs, materials, fabrication, dimensioning with high safety margins;
- Recurrent testing, ageing management, preventive maintenance, etc.;
- Isolation equipment;
- Additional retention functions (filters, water layers, pressure differences);
- Shielding materials (concrete, water layer, etc.).

Radiological Safety Functions

During Normal NPP operation

- **Release limits;**
- **Direct exposure limits;**
  - As low as reasonably achievable (ALARA);
- **Continuous control and supervision of radioactive materials;**
- **Controlled and predetermined release paths;**

Design basis accidents

- **DBA specific release and exposure limits;**
- **Analysis of a potential release/exposure paths;**

Beyond design basis accidents (design extension)

- **Minimize radiological impact within and outside the plant (mitigative measures).**

Redundancy

A number of safety functions are designed for redundancy, i.e. at least one more safety system is capable of providing the requested safety function;

In most reactor designs, the following systems are designed against single failure;

- Fast reactor shutdown;
- Residual heat removal from the core;
- Emergency core cooling;
- Containment isolation;
- Containment heat removal;
- Containment atmosphere control and clean-up.

Diversity

Common Cause Failures (CCF) bypass redundancy;

CCF important contributor to accident scenarios;

Countermeasure: Diversity;

- ***Redundant*** **Systems or Components (2 or more) for a safety function with**
- ***Different*** **Attributes;**
  - Operating conditions (high pressure / low pressure);
  - Physical methods (transducers for pressure, temperature, flow rate);
  - Working principles (electric / combustion motor);
  - Manufactures;
  - Design teams;
- **Low Likelihood for CCF;**
- **Growing importance (actuation of protection system, pilot valves, emergency power supply, service water supply, etc.).**

Nuclear Safety Evolution

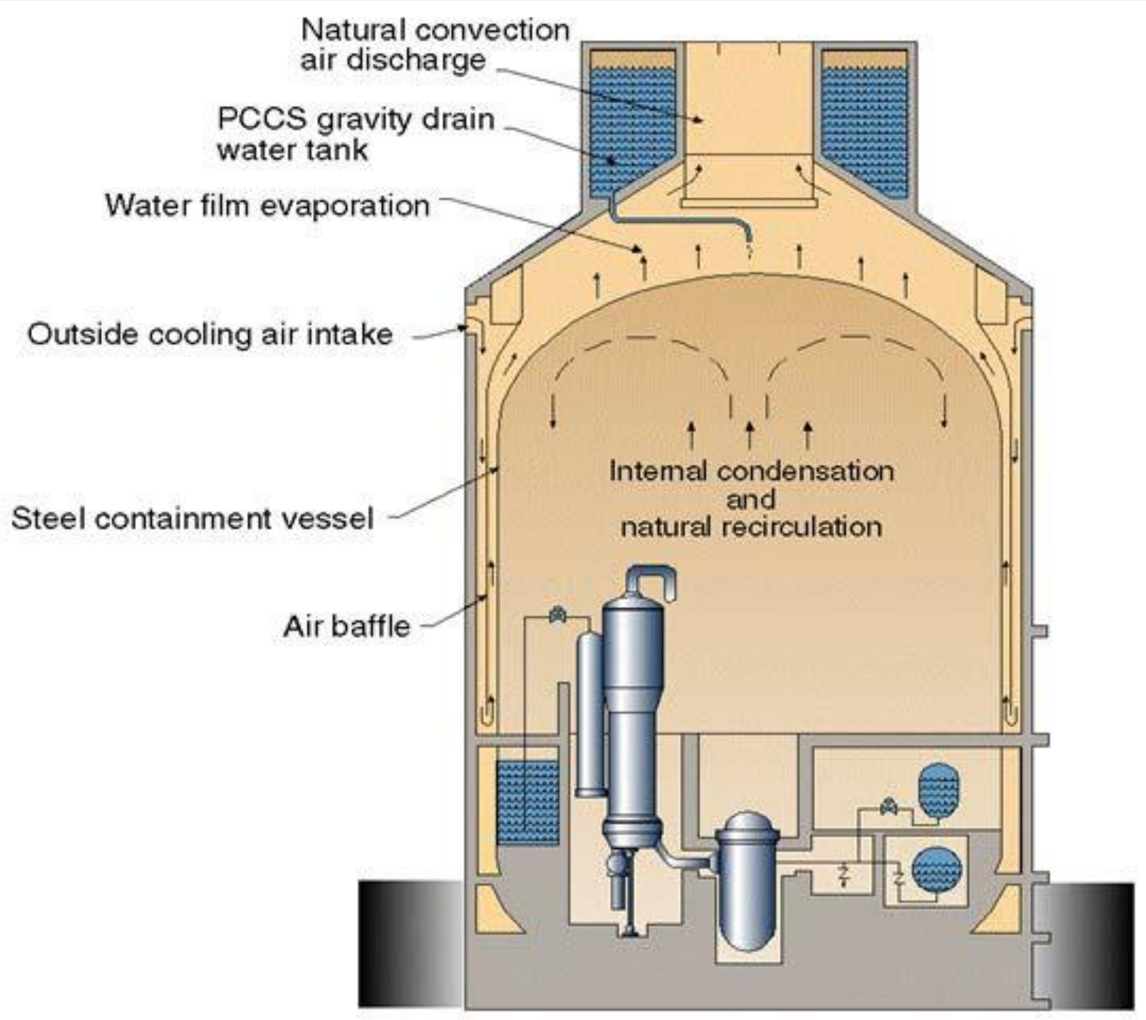
Design Safety Requirements have increased:

- **Separation of redundant trains;**
  - e.g. fire confinement;
- **Passive safety systems;**
  - e.g. Physical processes instead of powered (active) technical components;
- **Protection against hazards;**
  - Natural hazards, e.g. seismic;
  - Man-made hazards, e.g. plane crash;
- **Exclusion of core melt accidents;**
  - Generation IV reactors.

Passive Safety Systems Example – AP1000

Containment cooling relies on;

- Water inventory;
- Gravity;
- Natural circulation;
- Residual power.



[Figure from Westinghouse]

Postulated Initiating Events Definition (1/2)

In the design of a nuclear power plant, a systematic approach is applied to identify a comprehensive set of *Postulated Initiating Events (PIEs);*

All foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design;

The PIEs are identified on the basis of engineering judgment and a combination of *deterministic* (considers mechanistically what can go wrong) and *probabilistic* analysis (considers probability and can assign more weight to accidents with higher probability);

They include *all foreseeable failures* of structures, systems and components, as well as operating errors and possible failures arising from internal and external hazards;

Postulated Initiating Events Definition (2/2)

From these, *Design Basis Accidents* and *Design Basis Events* are selected for determining the boundary conditions which the plant must withstand, without radiation protection limits being exceeded;

Some accidents beyond these latter two groups are considered in the design, to further improve safety. These include also events with fuel damage. The events are called *'Design Extension Conditions'* (DEC) (also known as Beyond Design Basis Accidents (BDBAs)):

Initiating Events Categorisation – examples (1/3)

Principal effect on potential degradation **of fundamental safety functions leads to the following event categories, considered typically in the reactor;**

- **Increase in heat removal by the secondary side;**
- **Decrease in heat removal by the secondary side;**
- **Decrease in flow rate in the reactor coolant system;**
- **Increase in flow rate in the reactor coolant system;**
- **Anomalies in distributions of reactivity and power;**
- **Decrease in reactor coolant inventory;**
- **Radioactive release from a subsystem or component;**

Initiating Events Categorisation – examples (2/3)

Grouping by *principal cause*

- Control rod malfunctions;
- Interfacing system LOCA, ISLOCA;
- Loss of power supply;
- Anticipated transient without scram;
- External event (seismic, flooding etc.).

Initiating Events Categorisation – examples (3/3)

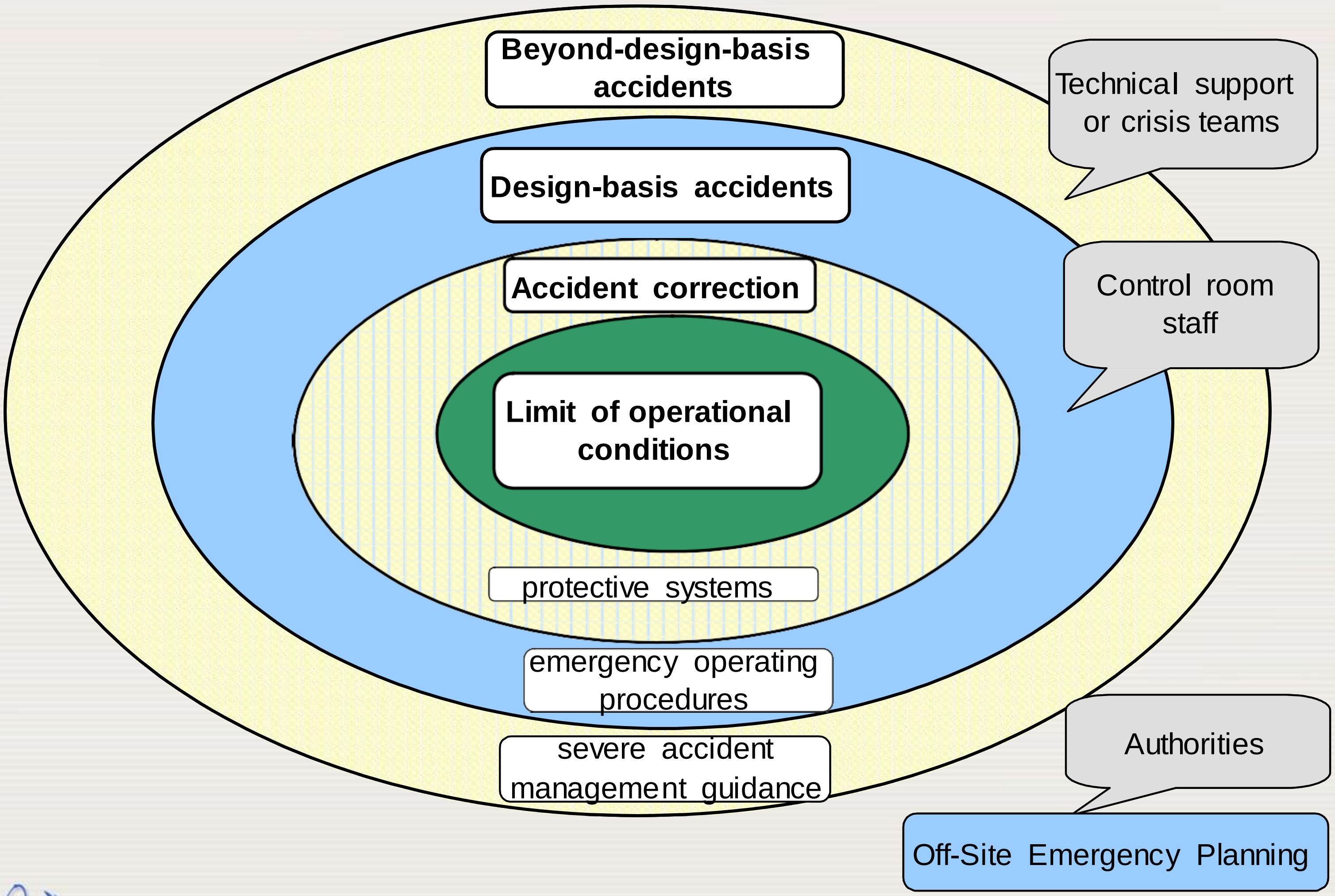
Grouping by *postulated initial event from internal cause;*

- **Pipe whipping (due to pipe failures);**
- **Fluid jet impingement forces (due to pipe failures);**
- **Internal flooding and spraying (due to leaks or breaks of pipes, pumps, valves);**
- **Internal missiles from pipe breaks or due to failure of rotating components;**
- **Load drop (e.g. fuel cask);**
- **Internal explosion;**
- **Fire.**

Examples of initiating event from *operating experience;*

- **Data for all unexpected reactor trips during power operation at US commercial nuclear power plants are yearly reviewed and categorized by the NRC. OECD, IAEA etc. compile lists of nuclear incidents and accidents worldwide.**

Design Basis – coupling with defence in depth (1/2)



Accident Scenario Classifications (1/2)

These span from normal operation to design extension conditions:

- ***Normal operation*, covering approach to criticality, start-up, power operation (steady-state and load following), hot standby, hot shutdown and cold shutdown (latter may have open RCS and containment);**
- ***Anticipated operational occurrences*, expected during plant life;**
  - An operational process deviating from normal operation which is expected to occur once or several times during the operating lifetime of the power plant but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety nor lead to accident conditions.
- ***Design basis accidents*, not expected to occur during plant life, but postulated to occur;**
  - Accident conditions against which an NPP is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits. The accidents are not expected to occur during plant life, but are postulated to occur to set the design basis.

Accident Scenario Classifications (2/2)

- ***Design extension conditions*, unlikely**
  - Accident conditions more severe than those of a DBA, not expected during plant life and very unlikely to happen. DECs are selected conditions beyond the DBAs/DBEs, for which the NPP still shall have provisions to prevent unacceptable radiological consequences, to the extent practical. A DEC may or may not involve core degradation.
- ***Severe accidents*, remote;**
  - An accident more severe than DBA and involving significant core / fuel degradation.

Instrumentation and Control – use in severe accidents

The instrumentation and control in presently operating plants have not been designed to operate under severe accident conditions.

Some not even under DBA conditions. For example, the steam generator level measurement may change at elevated pressure in the containment and usually does not compensate for this error.

Therefore, the plant parameters needed for severe accident management measures should be identified and it should be checked whether these parameters are available from the instrumentation in the plant, notably under severe accident and environmental conditions for the instruments.

Hence, the qualification of all relevant instruments should be recognized that, in order to obtain the required information, the equipment may need to operate well beyond its qualified range. Alternative instrumentation should be identified where the primary instrumentation is not available or not reliable. For instruments still available, it should be checked how much the measured parameters may deviate from their values under nominal conditions.

Conclusions

A summary of the basic concepts of nuclear safety has been presented, covering PWR, BWR and PHWR systems, in particular:

- Basic facts
- Fundamental safety principles
- Defence-in-depth
- Safety functions
- Initiating events

Plant features and behaviour have also been considered;

- Basic elements
- Structures, symbols and components
- Accident scenario classifications
- Acceptance criteria
- Plant operation and configuration
- Instrumentation and control