Budapest University of Technology and Economics
Faculty of Transportation Engineering and Vehicle Engineering
Department of Control for Transportation and Vehicle Systems

Nuclear Safety Basics

Introduction to the goals and terminology of Nuclear Safety

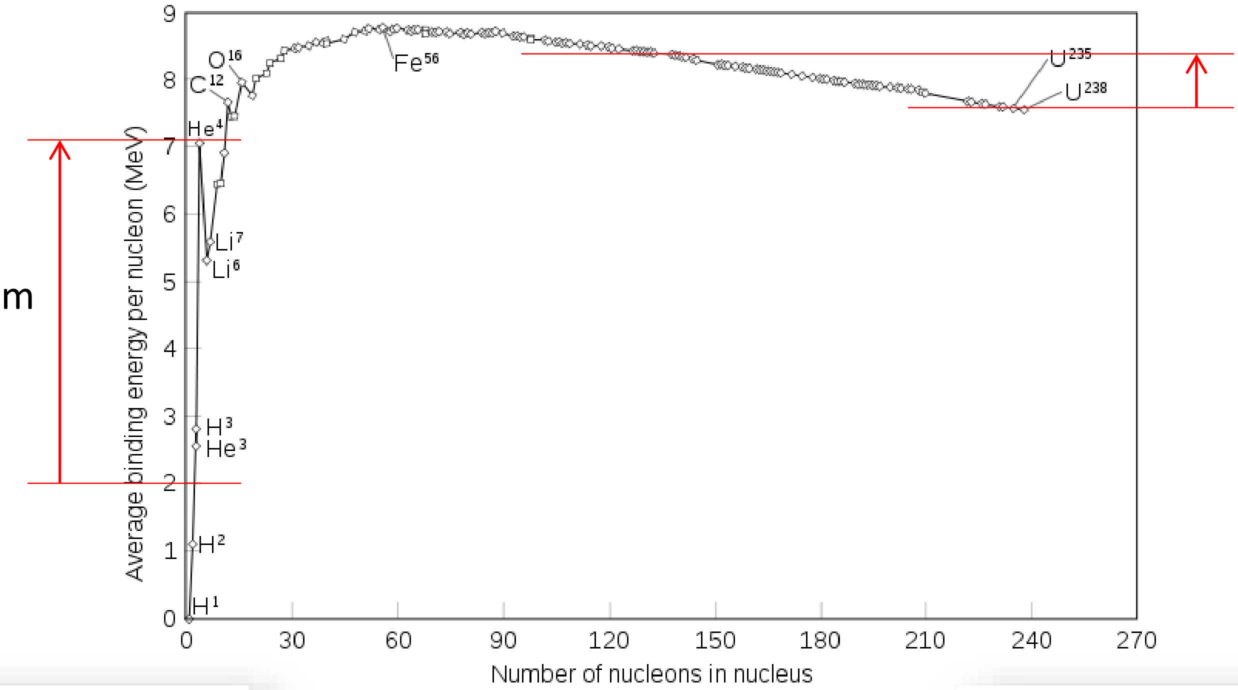
Nuclear Power Generation

Introduction to Nuclear Energy and Nuclear Power Plants

Nuclear Power — Is it even necessary?

- Fossil fuel power plants
  - burn carbon fuels such coal, oil or gas to generate steam driving large turbines that produce electricity
  - non-renewable fuel: oil depletes soon, gas next, carbon later
  - they produce large amounts carbon dioxide, which causes climate change
  - they increase background radiation
- Large hydro power plants
  - water from the dams flows through turbines to generate electricity
  - no greenhouse gas emissions
  - impact on the ecology around the dam
  - the number of sites suitable for new dams is limited
- Other renewables
  - wind, solar and small scale hydro produce electricity with no greenhouse gas emissions
  - higher cost than other forms of generation, often requiring subsidies
  - they do not produce electricity predictably or consistently
  - they have to be backed up by other forms of electricity generation

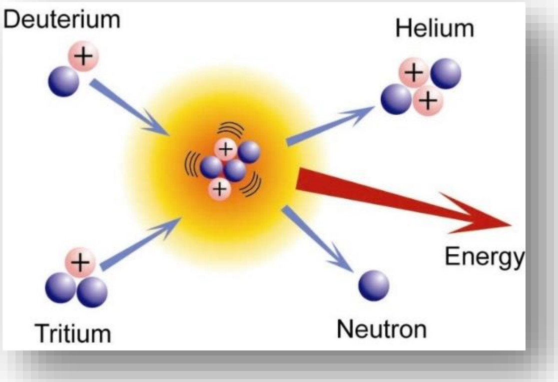
The Two Sources of Nuclear Energy Production



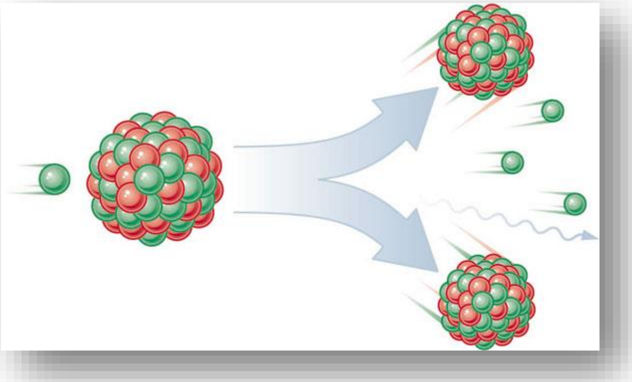
Energy yield from nuclear fission

Energy yield from nuclear fusion

Fusion



Fission

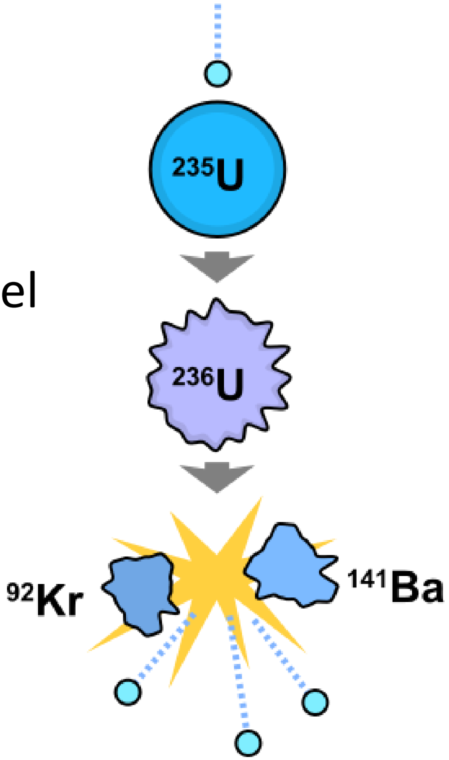


Comparison of Fission and Fusion

	Fission	Fusion
Mechanism	splitting of a large atom into two or more smaller ones	fusing of two or more lighter atoms into a larger one
Conditions	criticality (prompt subcriticality), moderator, and coolant	high density, high temperature (plasma), precise control
Energy produced	much greater than conventional	3 or 4 times greater than fission
Byproducts	highly radioactive isotopes, long decay time, large residual heat	some helium and tritium (short half-life, very low decay energy)
Nuclear waste	byproducts, structural materials	structural materials (lower half-life)
Fuel	^{235}U (0.72%), ^{232}Th, possibly ^{238}U	^{2}H (deuterium) and ^{3}H (tritium)
Advantages	no greenhouse emissions, economical, highly concentrated fuel, intrinsically safe	no greenhouse emissions, very low amount of waste, abundant fuel, intrinsically safe, low risk
Disadvantages	high risk, radioactive waste	commercial application is far away

Controllability of Nuclear Fission

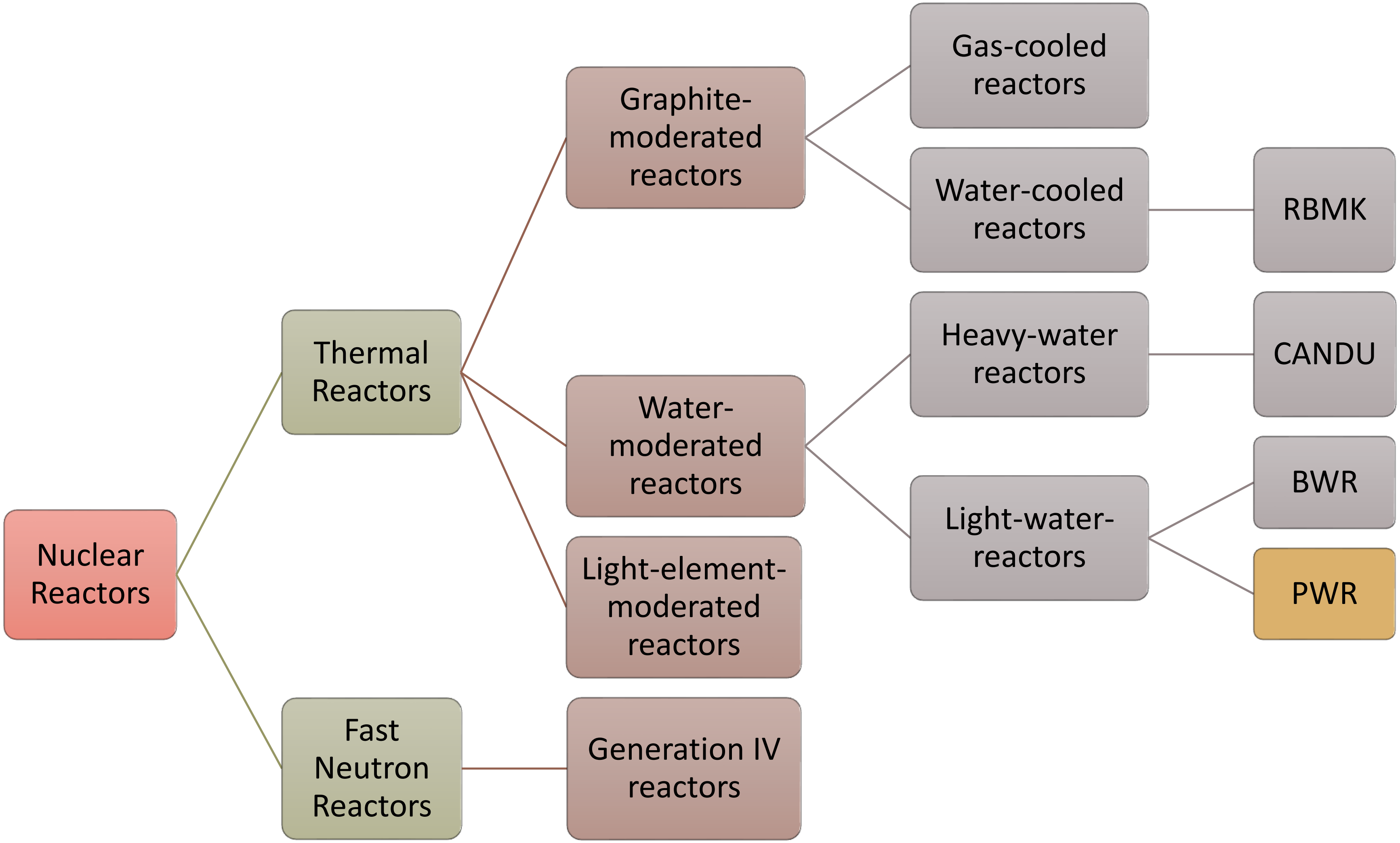
- Effective neutron multiplication factor (k) is the average number of neutrons from one fission to cause another fission
  - k < 1 (subcriticality): the system cannot sustain a chain reaction
  - k = 1 (criticality): every fission causes an average of one more fission, leading to a constant fission (and power) level
  - k > 1 (supercriticality): the number of fission reactions increases exponentially
- Delayed neutrons are created by the radioactive decay of some of the fission fragments
  - The fraction of delayed neutrons is called β
  - Typically less than 1% of all the neutrons in the chain reaction are delayed
- $1 \leq k < 1/(1-\beta)$ is the delayed criticality region, where all nuclear power reactors operate



Inherent Safety of Nuclear Power Plants

- Reactivity is an expression of the departure from criticality: $\rho = (k - 1)/k$
  - when the reactor is critical, $\rho = 0$
  - when the reactor is subcritical, $\rho < 0$
- The temperature coefficient (of reactivity) is a measure of the change in reactivity (resulting in a change in power) by a change in temperature of the reactor components or the reactor coolant
- The void coefficient (of reactivity) is a measure of the change in reactivity as voids (typically steam bubbles) form in the reactor moderator or coolant
- Most existing nuclear reactors have negative temperature and void coefficients in all states of operation

(A Few) Types of Nuclear Reactors



Nuclear Reactors

Thermal Reactors

Fast Neutron Reactors

Graphite-moderated reactors

Water-moderated reactors

Light-element-moderated reactors

Generation IV reactors

Gas-cooled reactors

Water-cooled reactors

Heavy-water reactors

Light-water-reactors

RBMK

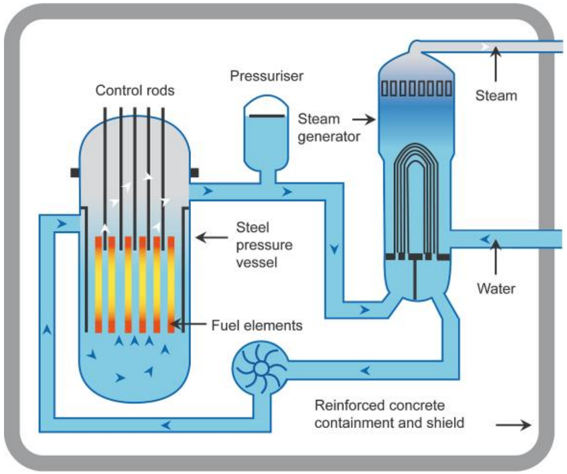
CANDU

BWR

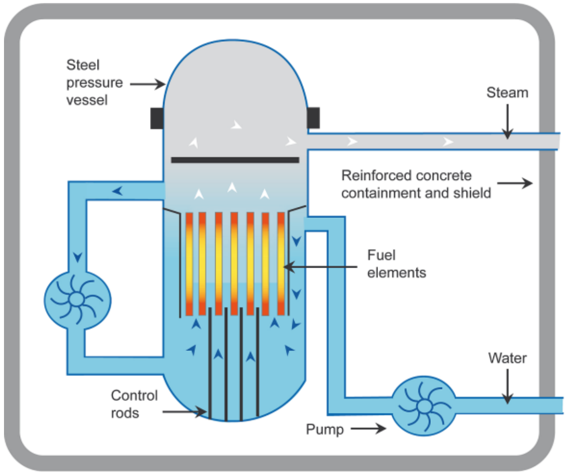
PWR

Typical Reactor Structures

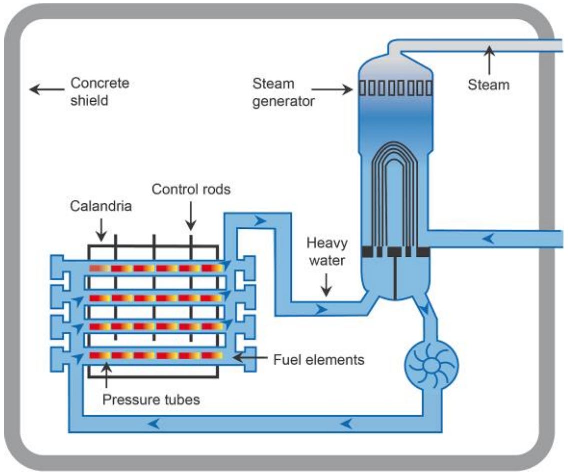
Typical Pressurized Light-Water Reactor (PWR)



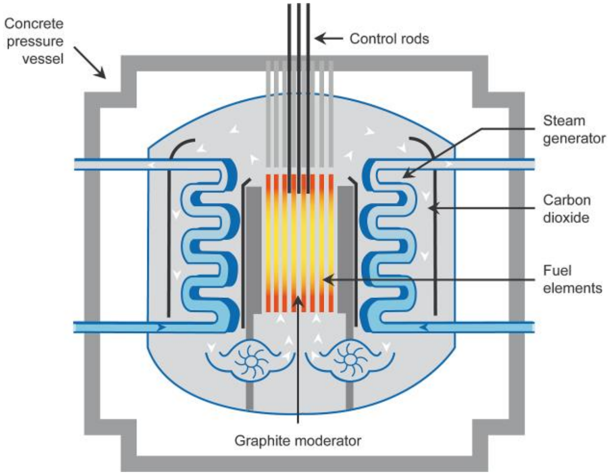
Typical Boiling Light-Water Reactor (BWR)



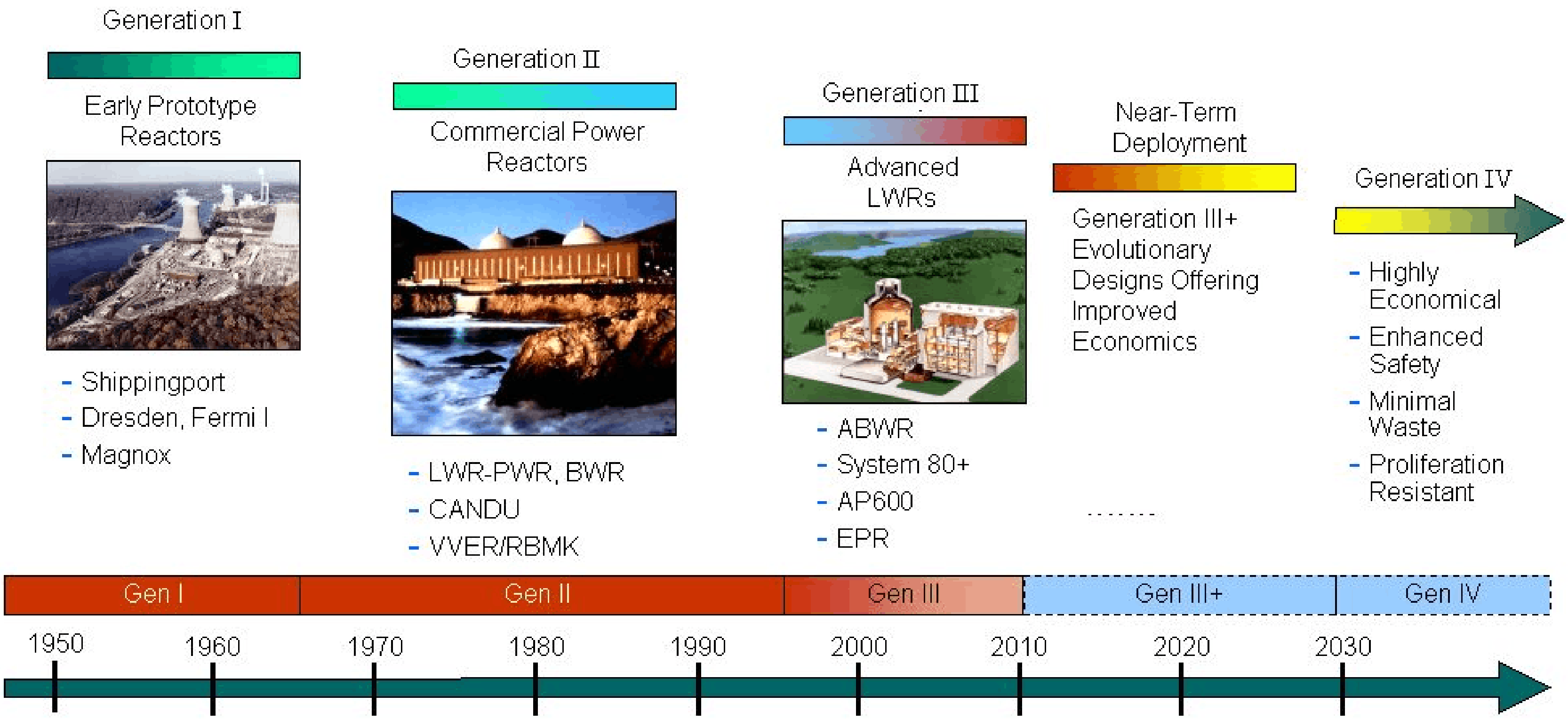
Typical Pressurized Heavy-Water Reactor (PHWR, CANDU)



Advanced Gas-Cooled Reactor (AGR)



Nuclear Reactor History and Generations



Generation I

Early Prototype Reactors

- Shippingport
- Dresden, Fermi I
- Magnox

Generation II

Commercial Power Reactors

- LWR-PWR, BWR
- CANDU
- VVER/RBMK

Generation III

Advanced LWRs

- ABWR
- System 80+
- AP600
- EPR

Near-Term Deployment

Generation III+ Evolutionary Designs Offering Improved Economics

....

Generation IV

- Highly Economical
- Enhanced Safety
- Minimal Waste
- Proliferation Resistant

- Generation II: class of commercial reactors built up to the end of the 1990s
- Generation III: development of Gen. II designs, improved fuel technology, superior thermal efficiency, passive safety systems, and standardized design
- Generation IV: nuclear reactor designs currently being researched, not expected to be available for commercial construction before 2030

Gen. II Water Moderated Reactor Types

Pressurized Water Reactor (PWR)

Cooled and moderated by high-pressure liquid water, primary and secondary loops

Boiling Water Reactor (BWR)

Higher thermal efficiency, simpler design (single loop), potentially more stable and safe (?)

Pressurized Heavy Water Reactor (PHWR)

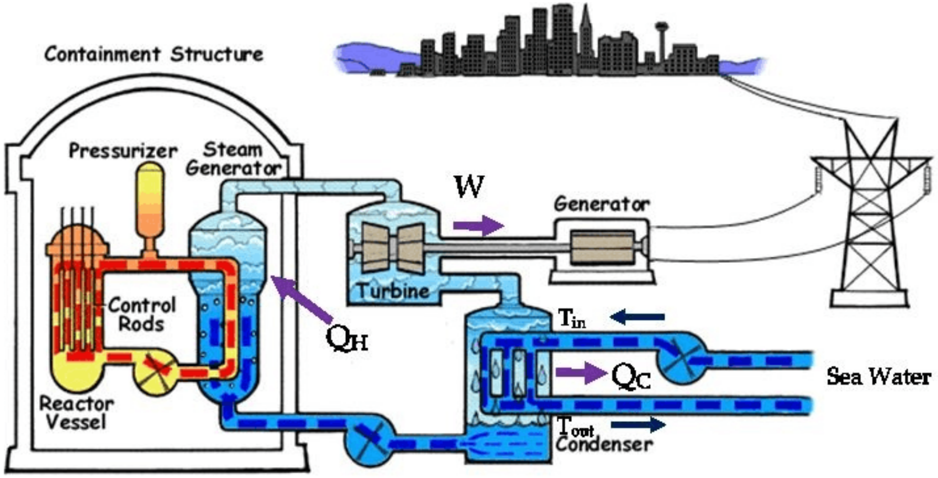
Heavy-water-cooled and -moderated pressurized-water reactors, fuel in tubes, efficient but expensive

High Power Channel Reactor (RBMK)

Water cooled with a graphite moderator, fuel in tubes, cheap, large and powerful reactor but unstable

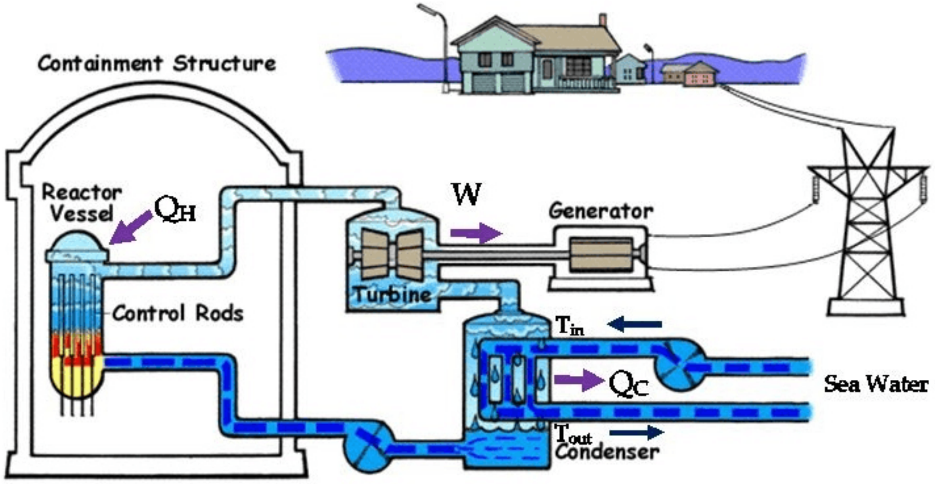
Common Light Water Moderated Reactors

Pressurized WR

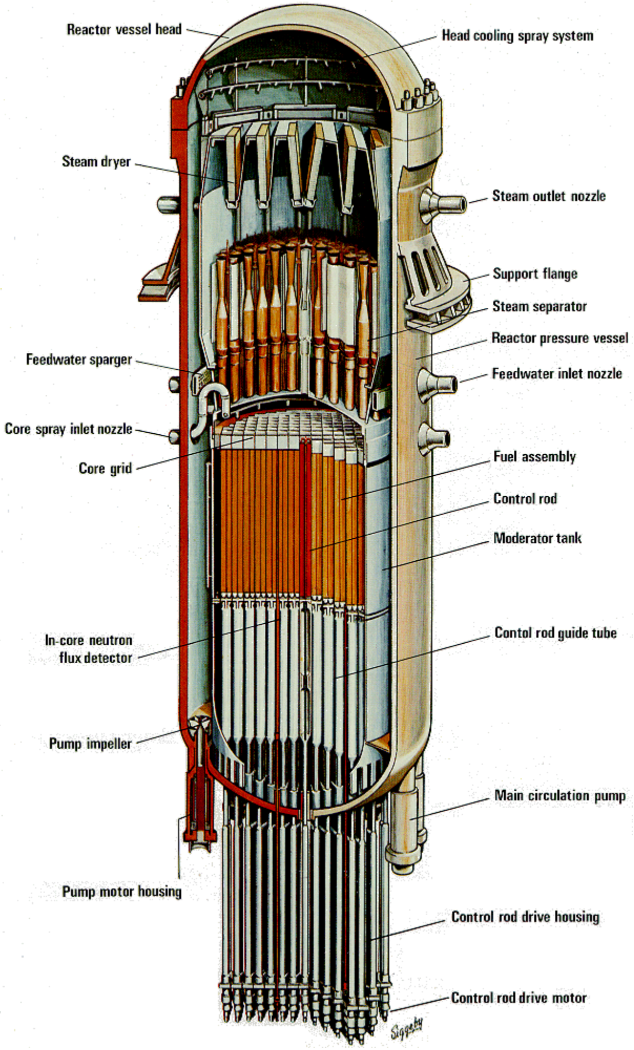


(a)

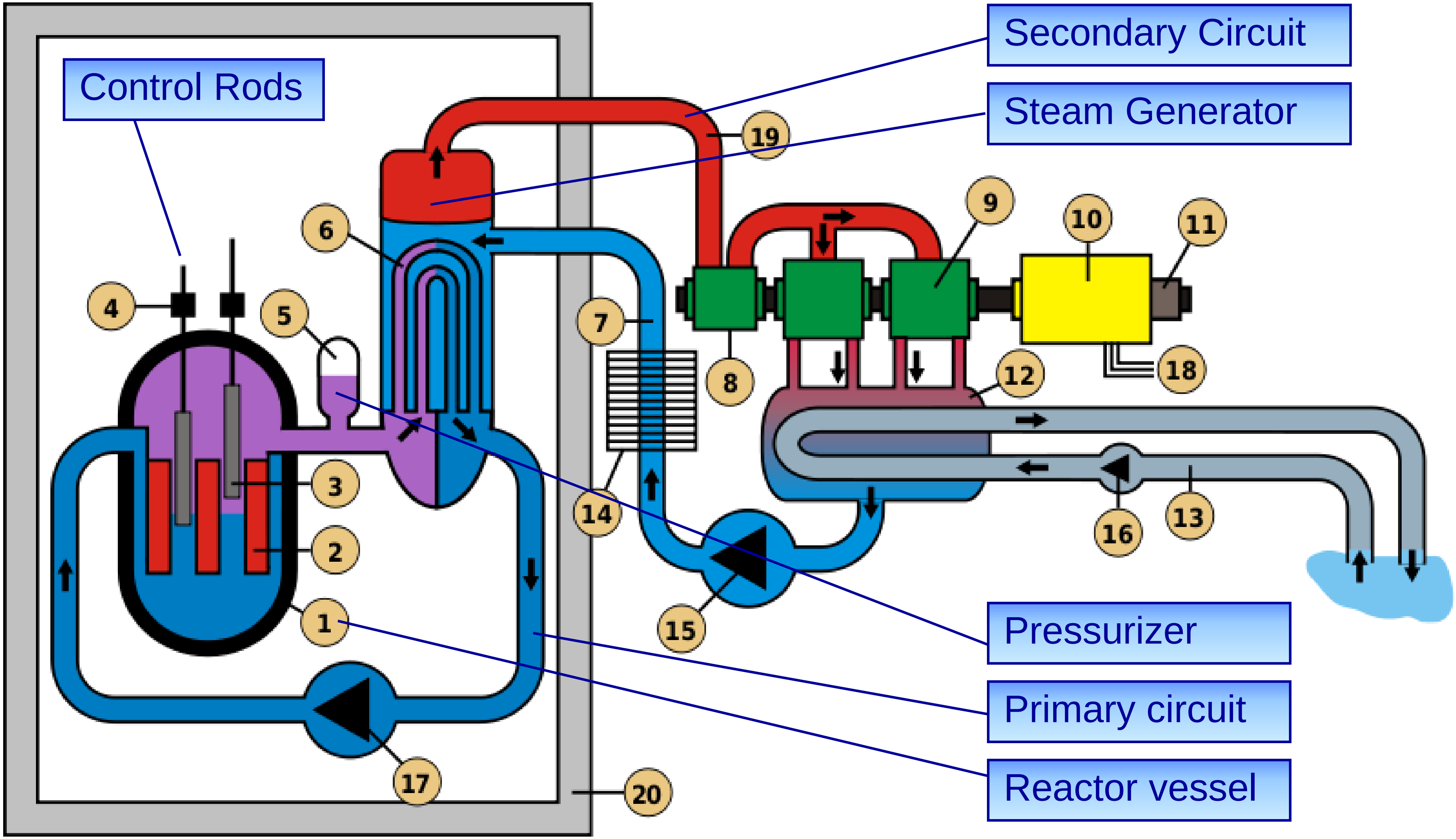
Boiling WR



(b)



Overview of a PWR nuclear power plant



Secondary Circuit

Steam Generator

Control Rods

Pressurizer

Primary circuit

Reactor vessel

Risk of Nuclear Installations

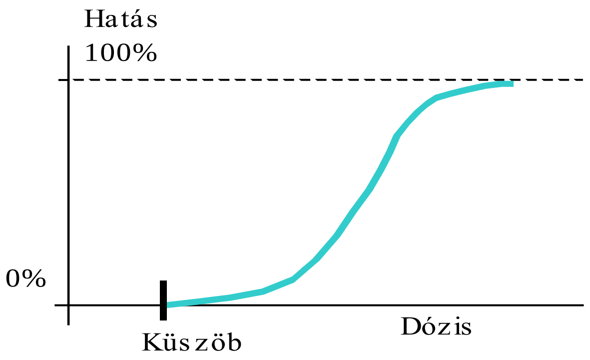
Using the Terms of the Functional Safety Concept

Functional Safety Concept: Risk

- Risk based approach for determining the target failure measure
  - Risk is a measure of the probability and consequence of a specified hazardous event occurring
  - There is no such thing as „Zero Risk“
- A safety-related system both
  - implements the required safety functions necessary to
    - achieve a safe state for the EUC or
    - to maintain a safe state for the EUC
  - is intended to achieve the necessary safety integrity for the required safety functions

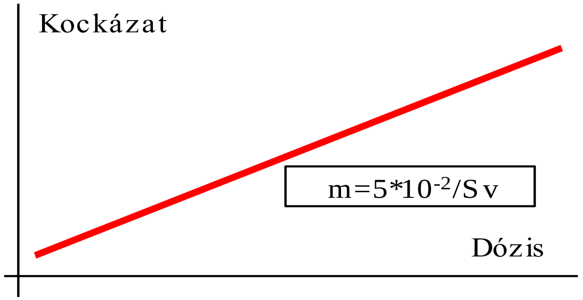
Consequence: Effects of Ionizing Radiation

Deterministic effect



- Natural radiation
    - Internal radiation: ^{40}K
    - External radiation
        - Background radiation
- TENORM
    - artificially increased background radiation

Stochastic effect



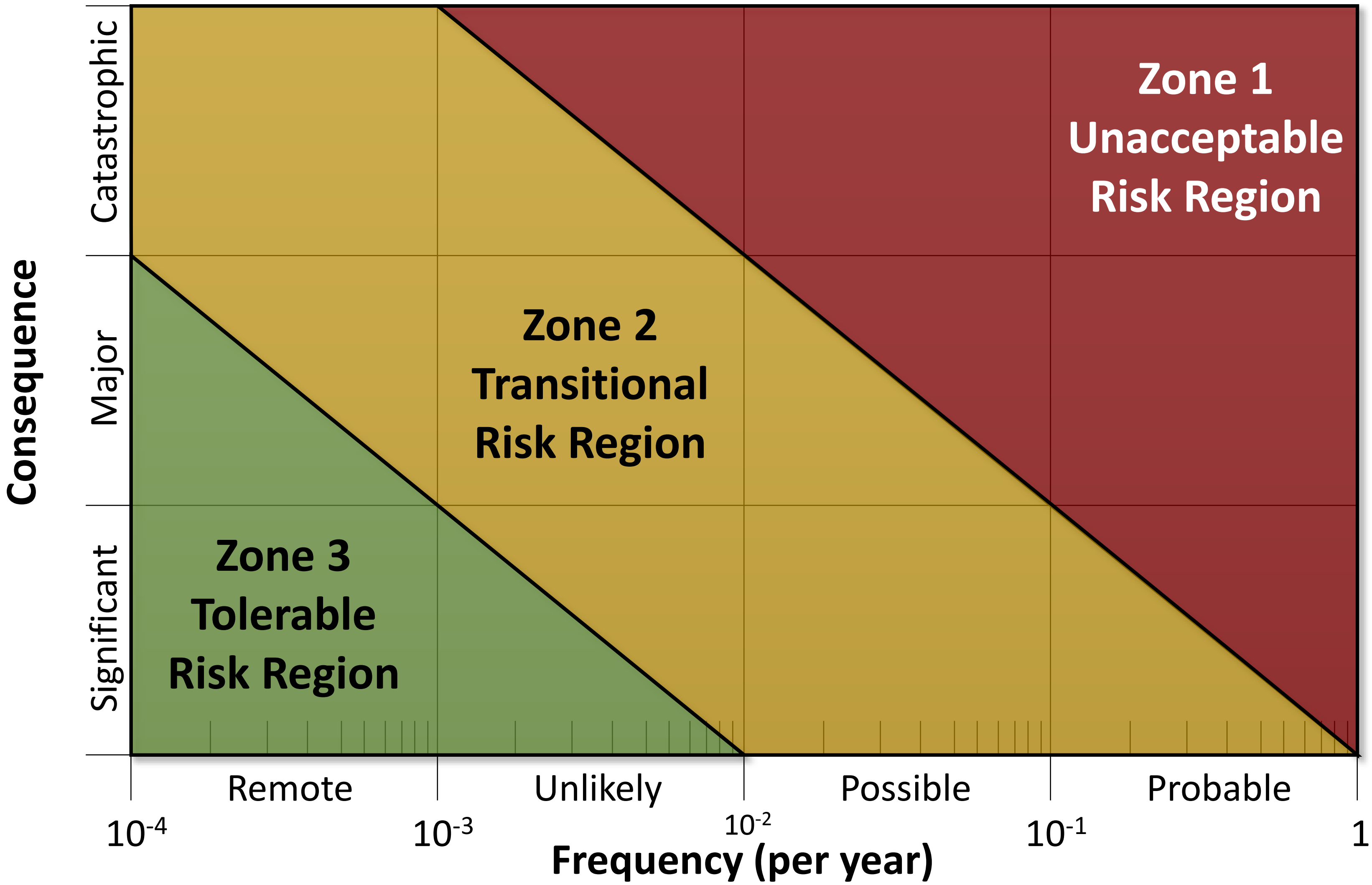
- Artificial radiation
    - Medical diagnosis and treatment
    - Industrial radiation sources
    - Nuclear tests
    - Nuclear waste

The Risk Assessment Framework

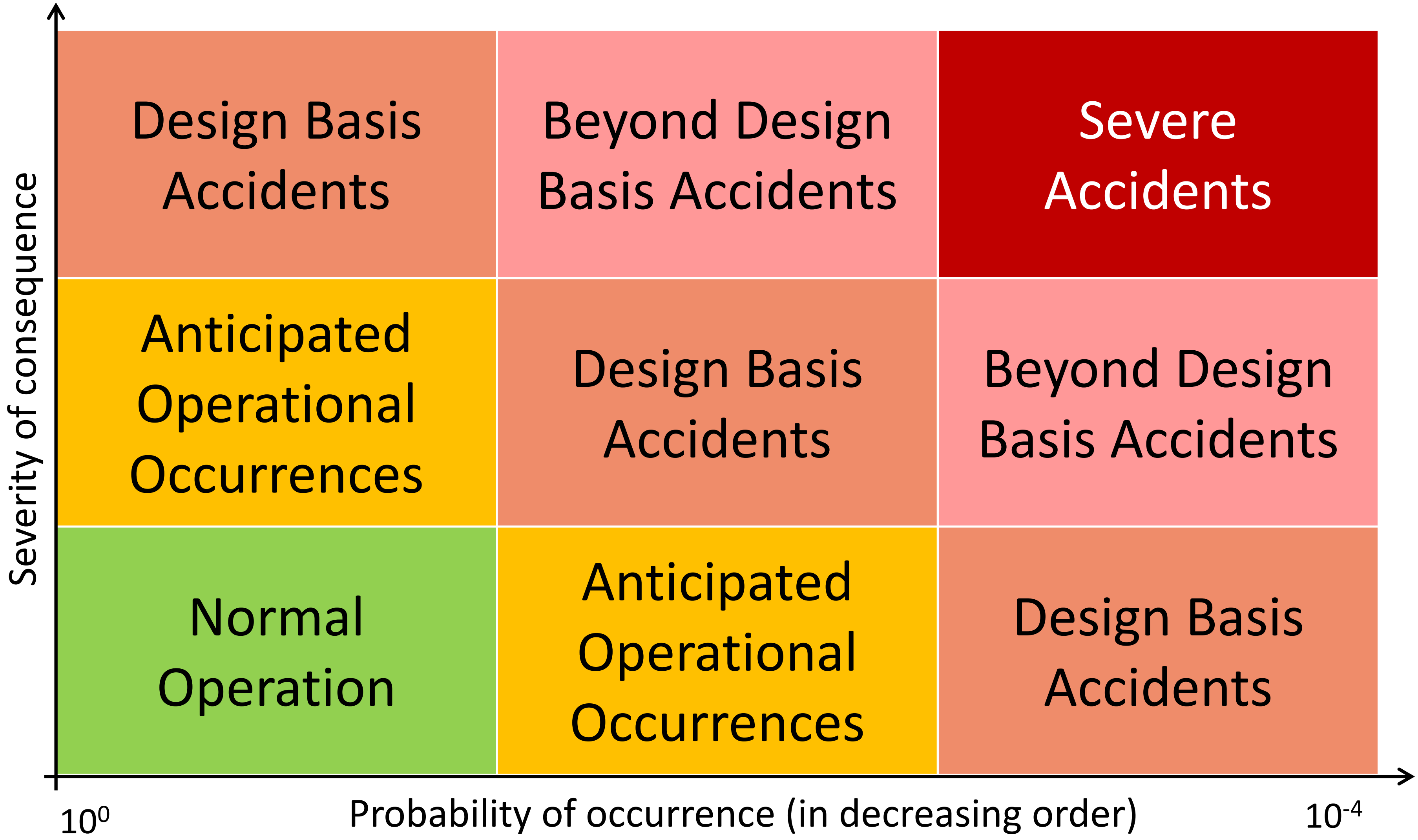
- The three main stages of Risk Assessment are:

1. Establish the tolerable risk criteria with respect to
    - the frequency (or probability) of the hazardous event
    - and its specific consequences
2. Assess the risks associated with the equipment under control
3. Determine the necessary risk reduction needed to meet the risk acceptance criteria
    - this will determine the Safety Integrity Level of the safety-related systems and external risk reduction facilities

Example Risk Bands for Tolerability of Hazards



Tolerable Risk of Nuclear Installations

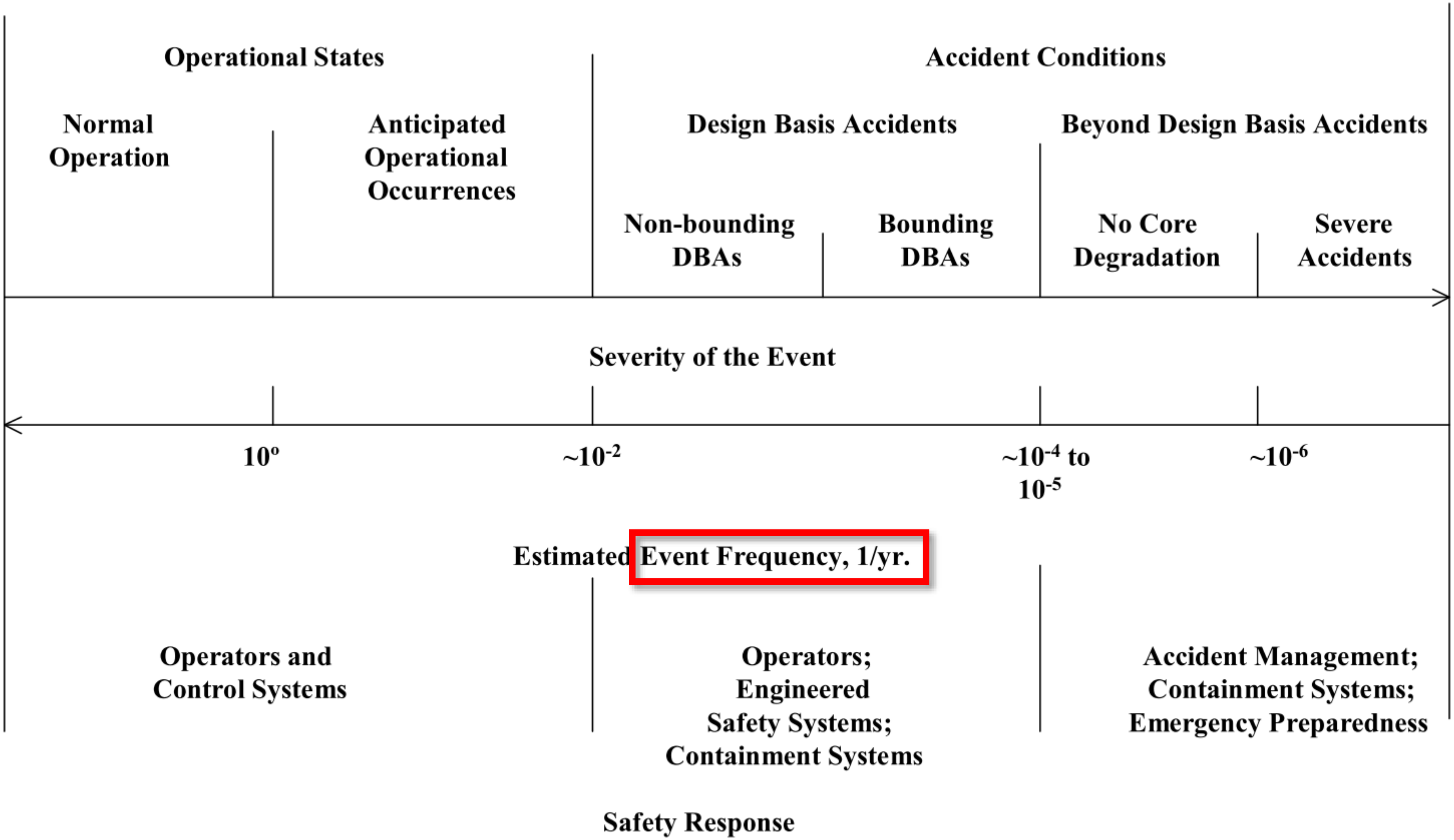


Design Basis Accidents	Beyond Design Basis Accidents	Severe Accidents
Anticipated Operational Occurrences	Design Basis Accidents	Beyond Design Basis Accidents
Normal Operation	Anticipated Operational Occurrences	Design Basis Accidents

Operational States and Transients of NPPs

- Normal Operational State
  - most probable, most frequent state
- Operational Transients aka.
  Anticipated Operational Occurrences (AOO)
  - highly probable operational occurrences, having a minor effect
  - good chance of multiple AOOs during operational life-time
- Design Basis Accidents
  - improbable accidents, these are included in the Design Basis
- Beyond Design Basis Accidents – Severe Accidents
  - extremely improbable accidents
  - the Design Basis of most existing units does not include BDBAs
  - this is changing, many former BDBAs became DBAs in the case of Generation III and Generation IV nuclear units

Classification of Events & Operating Conditions



Operational States

Normal Operation

Anticipated Operational Occurrences

Accident Conditions

Design Basis Accidents

Non-bounding DBAs

Bounding DBAs

Beyond Design Basis Accidents

No Core Degradation

Severe Accidents

Severity of the Event

10^{0}

$\sim 10^{-2}$

$\sim 10^{-4}$ to 10^{-5}

$\sim 10^{-6}$

Estimated Event Frequency, 1/yr.

Operators and Control Systems

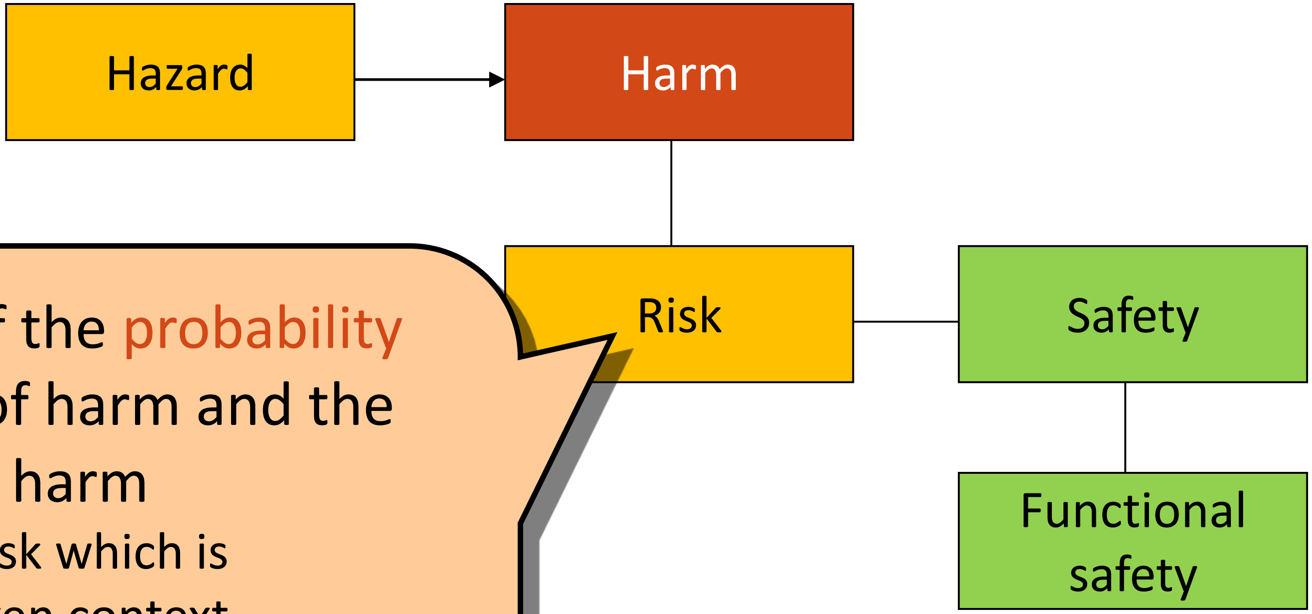
Operators; Engineered Safety Systems; Containment Systems

Accident Management; Containment Systems; Emergency Preparedness

Safety Response

Definition of Safety

- Central concepts: Hazard, risk and safety



Combination of the probability of occurrence of harm and the severity of that harm

- Tolerable risk: Risk which is accepted in a given context (based on the values of society)
- Residual risk: Risk remaining after protective measures have been taken

Postulated Initiating Events

- A postulated initiating event (PIE) is an "identified event that leads to an anticipated operational occurrence (AOO) or accident condition and its consequential failure effects."
  - All safety analysis, deterministic or probabilistic, begins with definition of a set of PIEs
- PIEs may be defined from various sources:
  - Formal analytical techniques, such as
    - Failure modes and effects analysis (FMEA), or
    - Hazards and operability analysis (HAZOP)
  - PIE lists developed for other, similar plants
  - Operating experience with other plants
  - Engineering judgement

Classification of PIEs

According to origin:

- Internal events
  - are those PIEs that arise
    - due to failures of systems, structures, components within the plant, or
    - due to internal human error, and
  - provide a challenge to internal safety systems.
- External events
  - are those PIEs that arise from
    - conditions external to the plant, such as natural phenomena, or
    - off-site human-caused events, and
  - provide a challenge to safety equipment and/or to plant integrity.

The Design Basis

- The design basis specifies the necessary capabilities of the plant to cope with a specified range of operational states and design basis accidents within the defined radiological protection requirements
- The design basis includes
  - the specification for normal operation,
  - plant states created by the PIEs,
  - the safety classification,
  - important assumptions and,
  - in some cases, the particular methods of analysis.

Identification of Internal Initiating Events

- Proper operation depends on maintaining the correct balance between
  - power production in the core
  - transport of energy in the reactor cooling system (RCS)
  - removal of energy from the RCS, and
  - production of electrical energy
- Thus, PIE categories may include:
  - change in heat removal from the RCS
  - change in coolant flow rate
  - change in reactor coolant inventory, including pipe breaks
  - reactivity and power distribution anomalies
  - release of radioactive material from a component or system

Identification of Internal Initiating Events

- Consider failures (including partial failures or malfunctions) of safety systems and components, as well as non-safety systems and components that impact safety function
- Consider consequences of human error:
  - Faulty maintenance
  - Incorrect settings or calibrations
  - Incorrect operator actions
- Include fires, explosions, floods which could cause failure of safety equipment
- Some events from outside the plant may be analyzed as internal events because of the nature of their impact
  - Loss of off-site power
  - Loss of component cooling water

Identification of External Initiating Events

External events can lead to an internal initiating event and failure of safety systems that provide protection.

- Naturally occurring events:
  - Earthquakes
  - Fires
  - Floods and other high water events
  - Volcanic eruptions
  - Extremes of temperature, rainfall, snowfall, wind velocity
- Human-caused events:
  - Aircraft crashes
  - External fires, explosions, and hazardous material releases

Nuclear Accidents

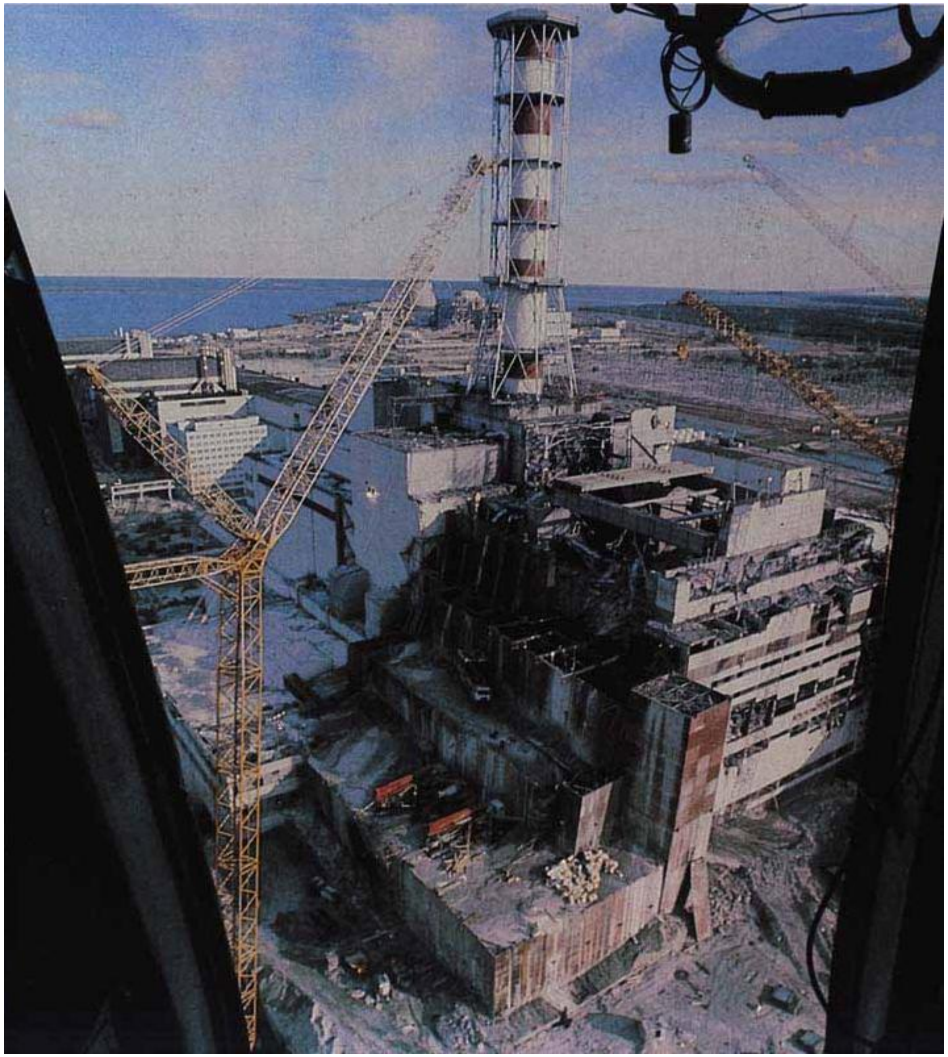
The Three Most Prominent Accidents in the History of Nuclear Power Generation, and Lessons Learned

Main Types of Nuclear Reactor Accidents

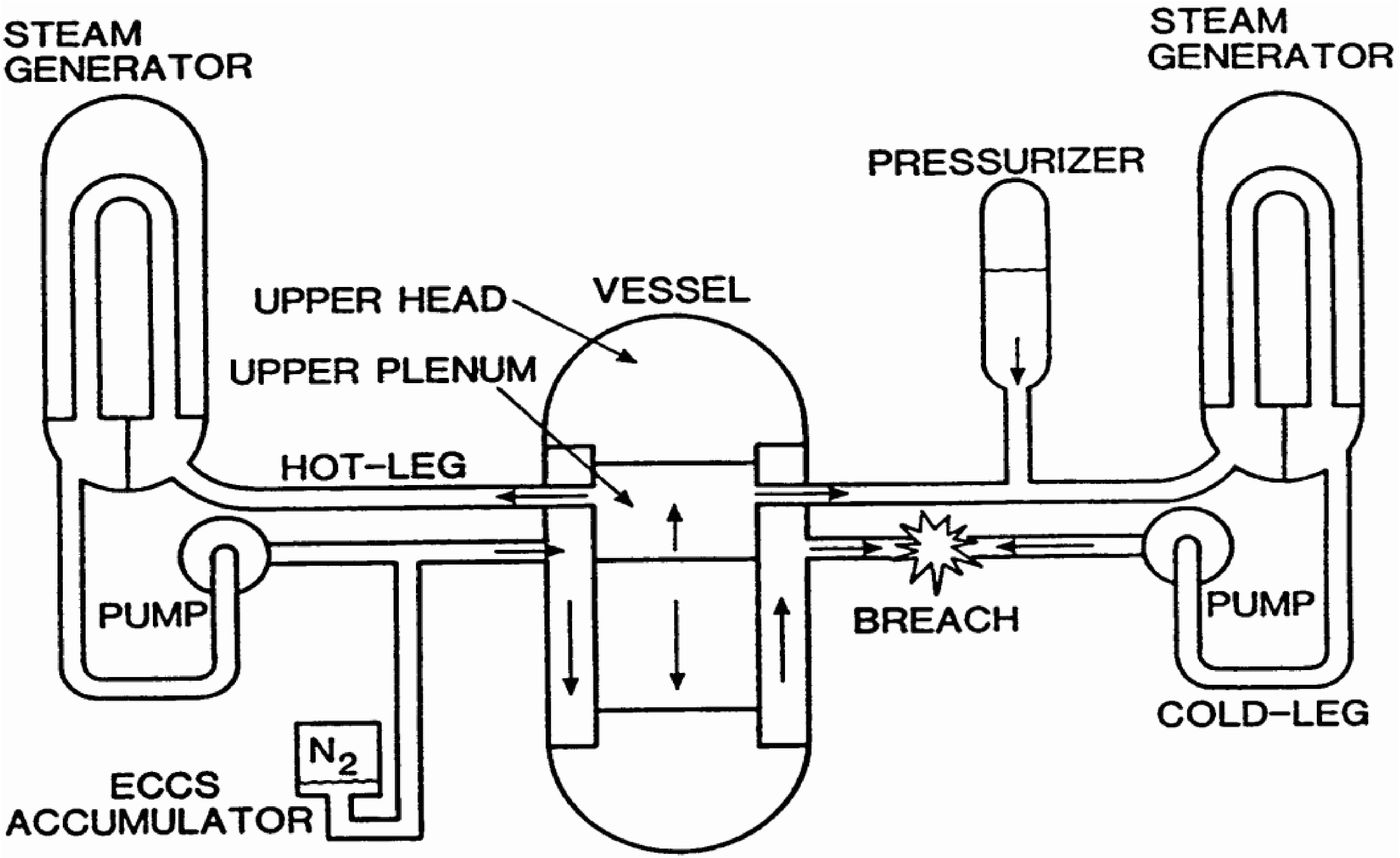
- Accident initiated by sudden reactivity increase (e.g. control rod ejection) that causes reactor runaway
  - RIA – Reactivity Initiated Accident
  - the nuclear chain reaction becomes uncontrollable
    - prompt supercritical reactor
- Accident initiated by insufficient cooling (e.g. due to loss of coolant)
  - the efficiency of heat removal from the core drops
  - the reactor core cooling is lost

  that can cause damage to the fuel cladding
  - LOCA – Loss of Coolant Accident
  - LOFA – Loss of Flow Accident
  - LOHA – Loss of Heat Sink Accident

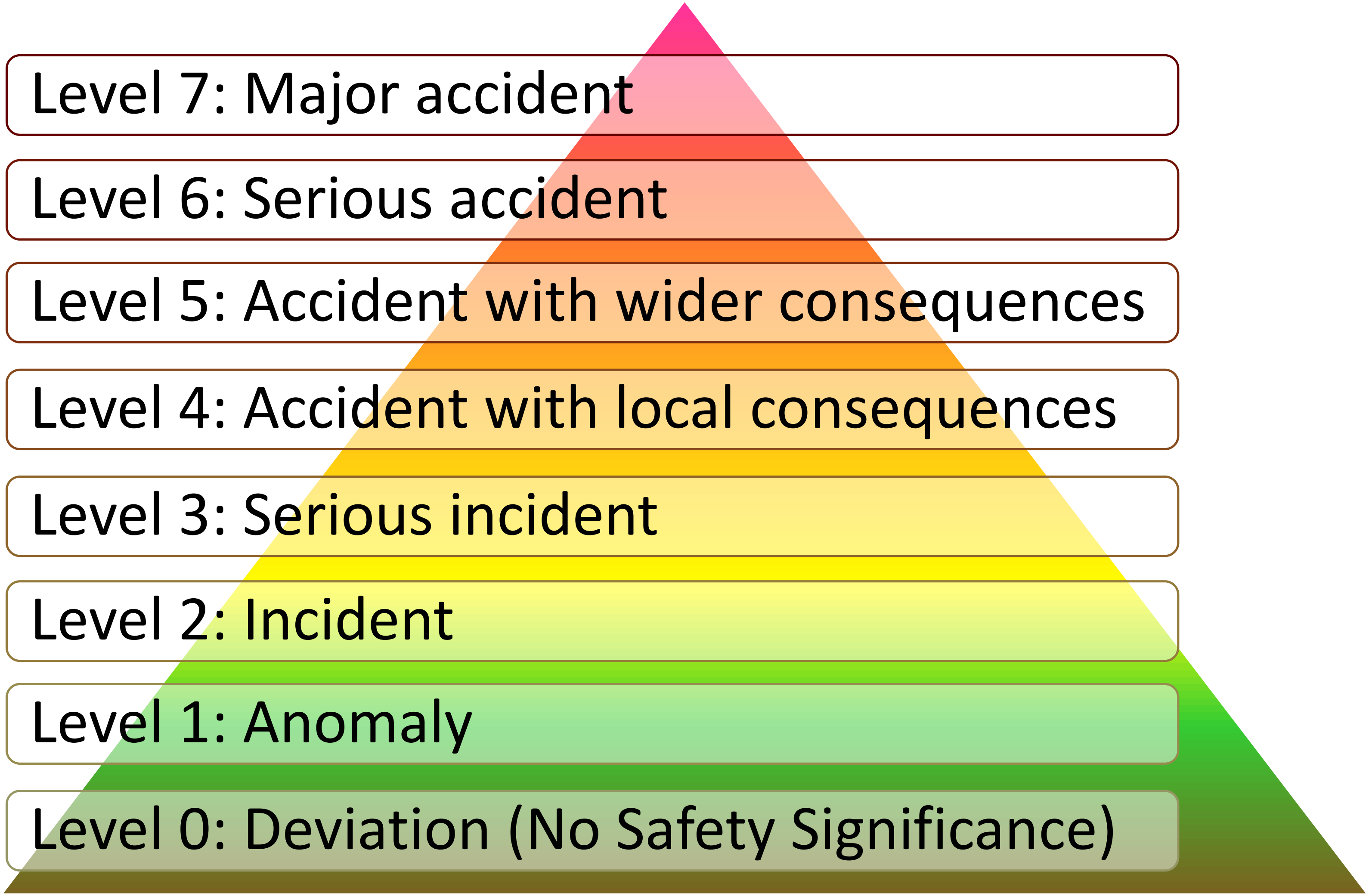
Reactivity Initiated Accident



Loss of Coolant Accident – LB LOCA



International Nuclear Event Scale (INES)



- Level 7: Major accident
- Level 6: Serious accident
- Level 5: Accident with wider consequences
- Level 4: Accident with local consequences
- Level 3: Serious incident
- Level 2: Incident
- Level 1: Anomaly
- Level 0: Deviation (No Safety Significance)

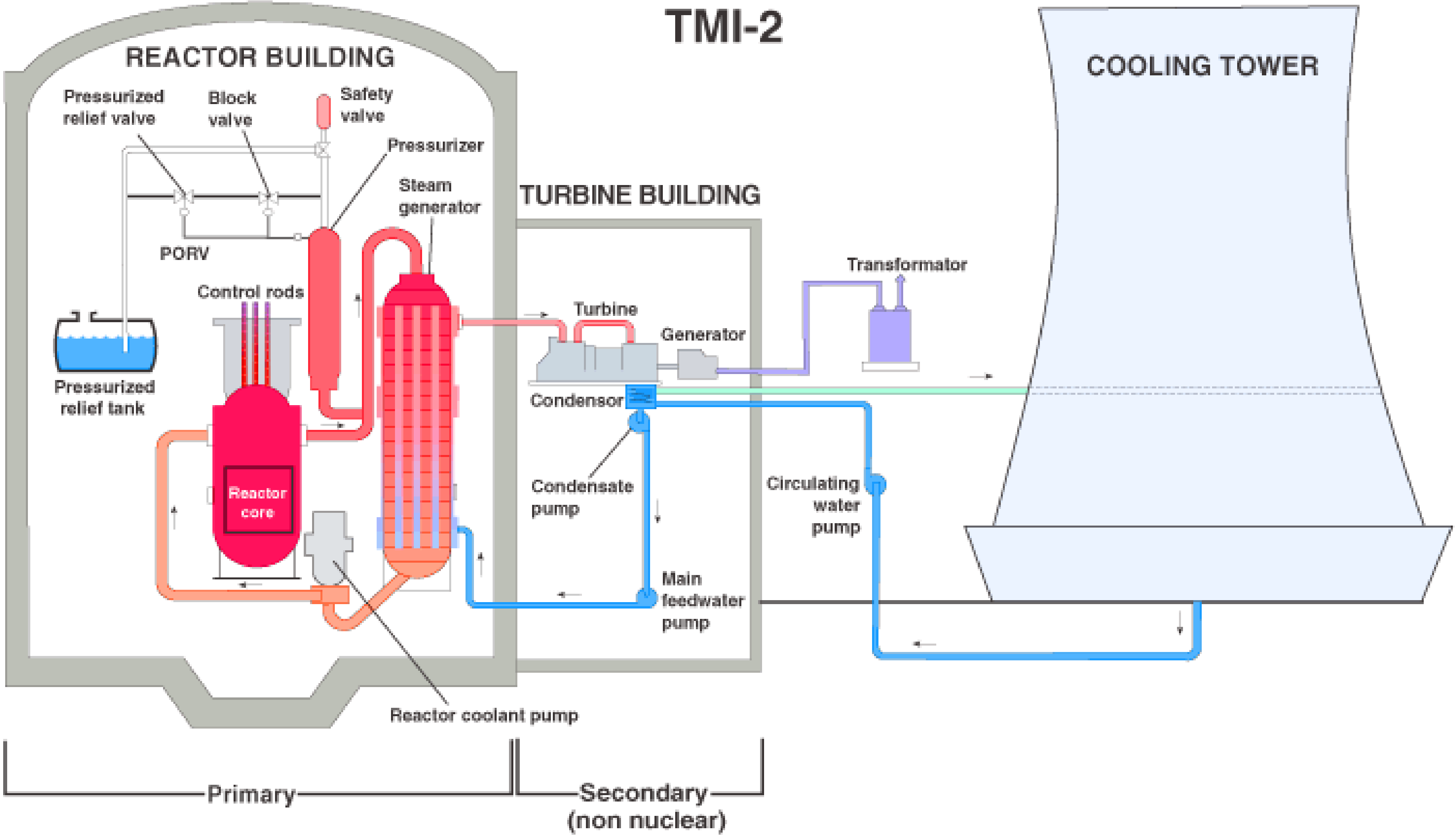
Details and Examples of the INES Scale

INES Level	People and Environment	Radiological Barriers and Control	Example
Level 7: Major accident	Major release of radioactive material Widespread effects		Chernobyl accident (Soviet Union), 26 April 1986 Fukushima accident
Level 6: Serious accident	Significant release of radioactive material		Kyshtym disaster at Mayak (Soviet Union), 29 September 1957
Level 5: Accident with wider consequences	Limited release of radioactive material Several deaths	Severe reactor core damage Significant release within installation	Three Mile Island accident (United States), 28 March 1979

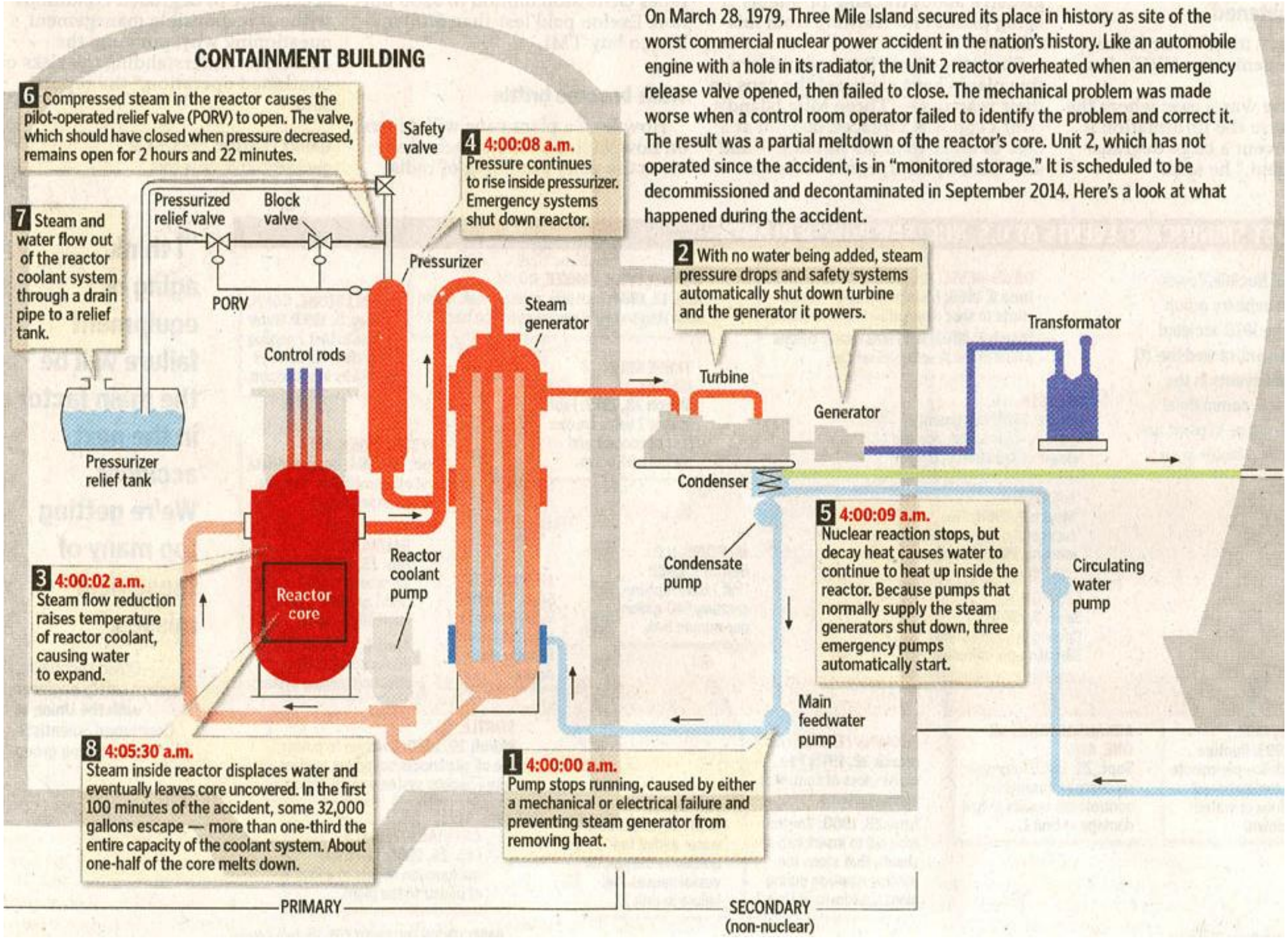
Three Mile Island Accident

- In 1979 at Three Mile Island nuclear power plant in USA a cooling malfunction caused part of the core to melt in the #2 reactor
    - A relatively minor malfunction in the secondary cooling circuit caused the temperature in the primary coolant to rise
    - This in turn caused the reactor to shut down automatically
    - A relief valve failed to close, but instrumentation did not reveal the fact
    - So much of the primary coolant drained away that the residual decay heat in the reactor core was not removed
    - The core suffered severe damage as a result
    - The operators were unable to diagnose or respond properly to the unplanned automatic shutdown of the reactor
    - Deficient control room instrumentation and inadequate emergency response training proved to be root causes of the accident
- Some radioactive gas was released a couple of days after the accident, but not enough to cause any dose above background levels
- There were no injuries or adverse health effects from the TMI accident

Three Mile Island Accident



Three Mile Island Accident



On March 28, 1979, Three Mile Island secured its place in history as site of the worst commercial nuclear power accident in the nation's history. Like an automobile engine with a hole in its radiator, the Unit 2 reactor overheated when an emergency release valve opened, then failed to close. The mechanical problem was made worse when a control room operator failed to identify the problem and correct it. The result was a partial meltdown of the reactor's core. Unit 2, which has not operated since the accident, is in "monitored storage." It is scheduled to be decommissioned and decontaminated in September 2014. Here's a look at what happened during the accident.

1 **4:00:00 a.m.** Pump stops running, caused by either a mechanical or electrical failure and preventing steam generator from removing heat.

2 With no water being added, steam pressure drops and safety systems automatically shut down turbine and the generator it powers.

3 **4:00:02 a.m.** Steam flow reduction raises temperature of reactor coolant, causing water to expand.

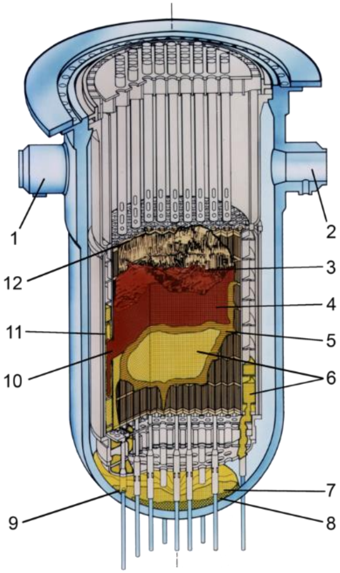
4 **4:00:08 a.m.** Pressure continues to rise inside pressurizer. Emergency systems shut down reactor.

5 **4:00:09 a.m.** Nuclear reaction stops, but decay heat causes water to continue to heat up inside the reactor. Because pumps that normally supply the steam generators shut down, three emergency pumps automatically start.

6 Compressed steam in the reactor causes the pilot-operated relief valve (PORV) to open. The valve, which should have closed when pressure decreased, remains open for 2 hours and 22 minutes.

7 Steam and water flow out of the reactor coolant system through a drain pipe to a relief tank.

8 **4:05:30 a.m.** Steam inside reactor displaces water and eventually leaves core uncovered. In the first 100 minutes of the accident, some 32,000 gallons escape — more than one-third the entire capacity of the coolant system. About one-half of the core melts down.

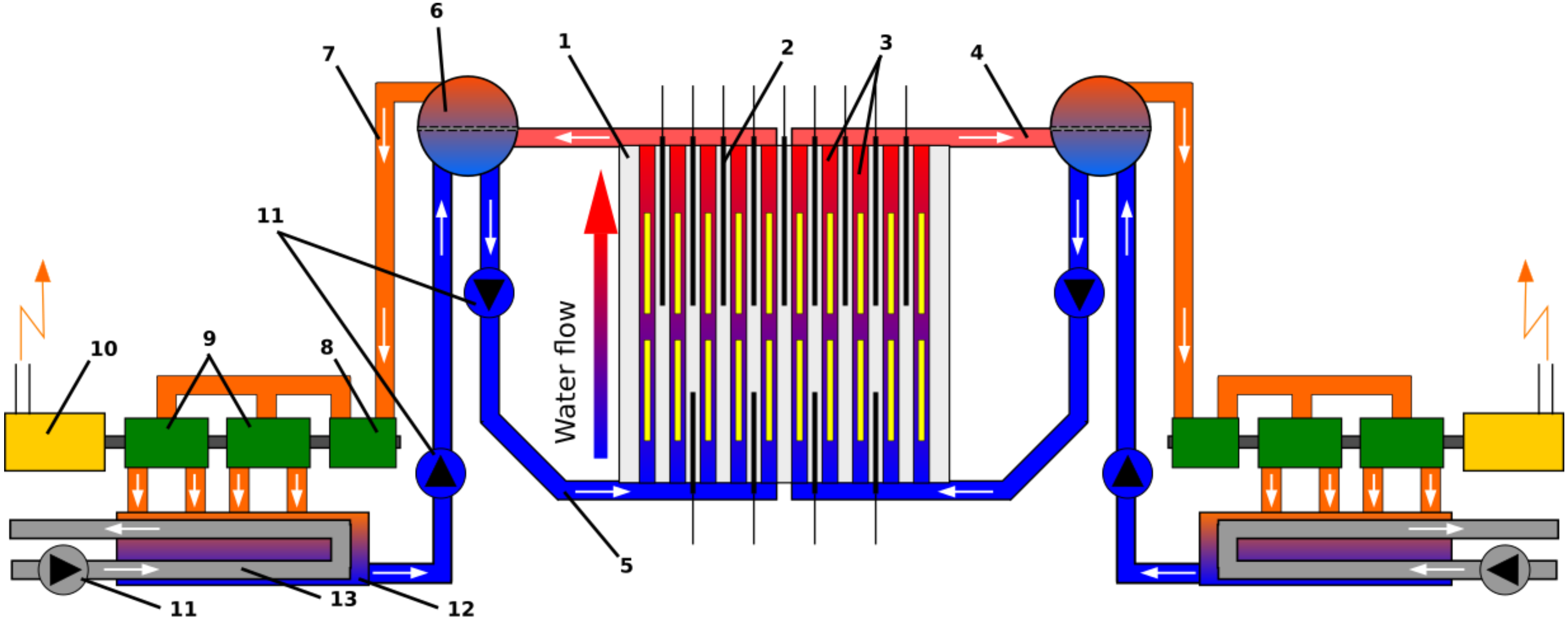


NRC graphic of TMI-2 core end-state configuration

Chernobyl Accident

- The Chernobyl accident in 1986 was the result of a flawed reactor design that was operated with inadequately trained personnel
  - The crew wanted to perform a test to determine how long turbines would spin and supply power to the main circulating pumps following a loss of main electrical power supply
  - A series of operator actions, including the disabling of automatic shutdown mechanisms, preceded the attempted test
  - By the time that the operator moved to shut down the reactor, the reactor was in an extremely unstable condition
  - A peculiarity of the design of the control rods caused a dramatic power surge as they were inserted into the reactor
    - The RBMK reactor can possess a positive void coefficient
  - The interaction of very hot fuel with the cooling water led to fuel fragmentation
  - Intense steam generation then spread throughout the whole core causing a steam explosion and releasing fission products to the atmosphere
  - A second explosion threw out fragments from the fuel channels and hot graphite
- The resulting steam explosion and fires released at least 5% of the radioactive reactor core into the atmosphere
- Two Chernobyl plant workers died on the night of the accident, and a further 28 people died within a few weeks as a result of acute radiation poisoning

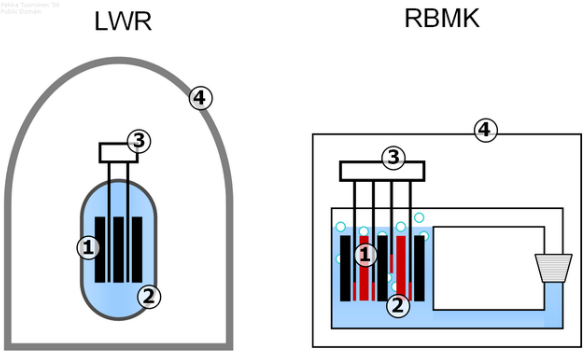
Schematic diagram of the RBMK reactor



Legend :

1. Graphite moderated reactor core
2. Control rods
3. Pressure channels with fuel rods
4. Water/steam mixture
5. Water
6. Water/steam separator
7. Steam inlet
8. High-pressure steam turbine
9. Low-pressure steam turbine
10. Generator
11. Pump
12. Steam condenser
13. Cooling water (from river, sea, etc.)

RBMK Reactor Hall



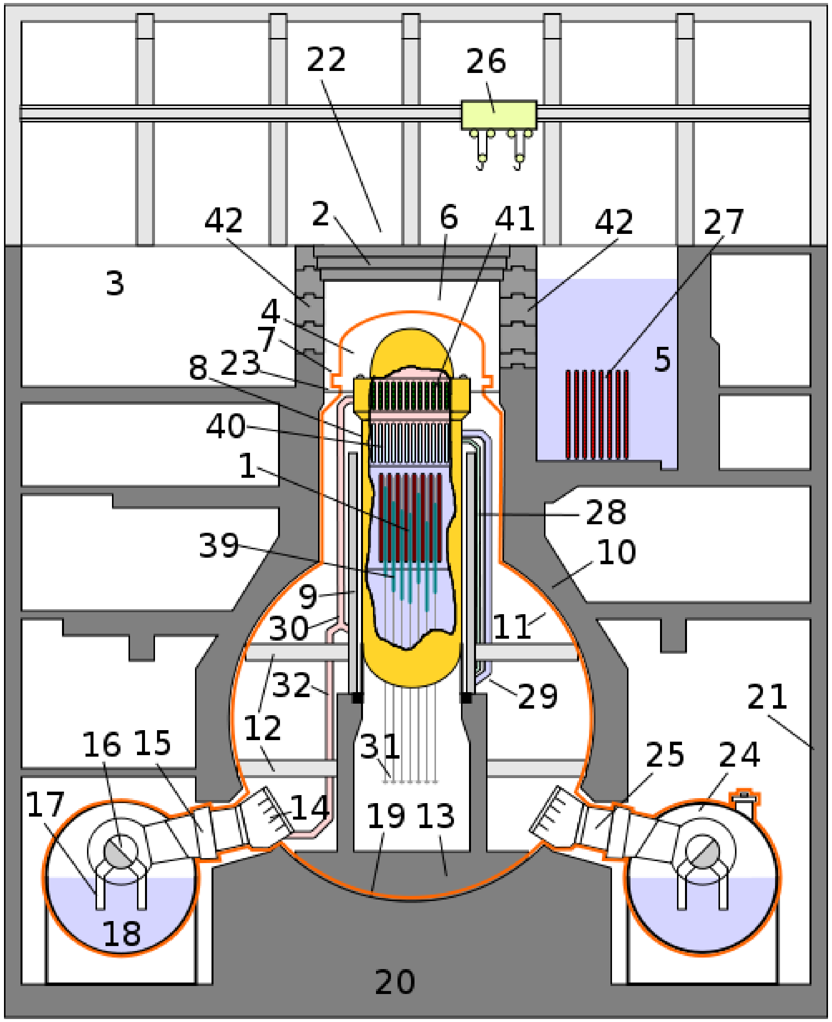
Major differences between the Chernobyl RBMK and the LWR:
1. The use of a graphite moderator in a water cooled reactor.
2. A positive steam void coefficient that made the power excursion possible, which blew the reactor vessel.
3. The control rods were very slow, taking 18-20 seconds to be deployed. The control rods had graphite tips that moderated, and thus increased the fission rate in the beginning of the rod insertion.
4. No reinforced containment building.

Chernobyl Accident

Fukushima Accident

- Following a major earthquake, a 15-metre tsunami disabled the power supply and cooling of three Fukushima Daiichi reactors, causing a nuclear accident on 11 March 2011
    - The reactors proved robust seismically, but vulnerable to the tsunami
    - This disabled 12 of 13 back-up generators on site and also the heat exchangers for dumping reactor waste heat and decay heat to the sea
    - The three units lost the ability to maintain proper reactor cooling and water circulation functions, all three cores largely melted in the first three days
- Rated 7 on the INES scale, due to high radioactive releases over days 4 to 6
- After two weeks the three reactors (units 1-3) were stable with water addition but no proper heat sink for removal of decay heat from fuel
- By July they were being cooled with recycled water from the new treatment plant, and official 'cold shutdown condition' was announced in mid-December
- Apart from cooling, the basic ongoing task was to prevent release of radioactive materials, particularly in contaminated water leaked from the three units
- There have been no fatalities linked to short term overexposure to radiation in the nuclear accident, but over 100,000 people had to be evacuated from their homes

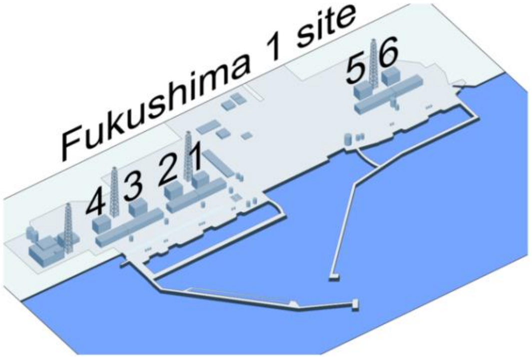
General Electric BWR Mark I containment



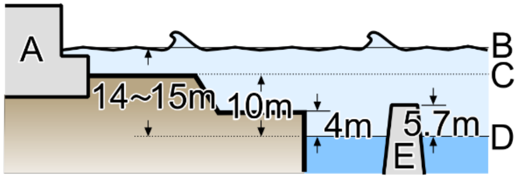
Cross-section sketch of a typical BWR Mark I containment, as used in Units 1 to 5.

The reactor core (1) consists of fuel rods and moderator rods (39) which are moved in and out by the device (31). Around the pressure vessel (8), there is an outer containment (19) which is closed by a concrete plug (2). When fuel rods are moved in or out, the crane (26) will move this plug to the pool for facilities (3). Steam from the dry well (11) can move to the wet well (24) through jet nozzles (14) to condense there (18). In the spent fuel pool (5), the used fuel rods (27) are stored.

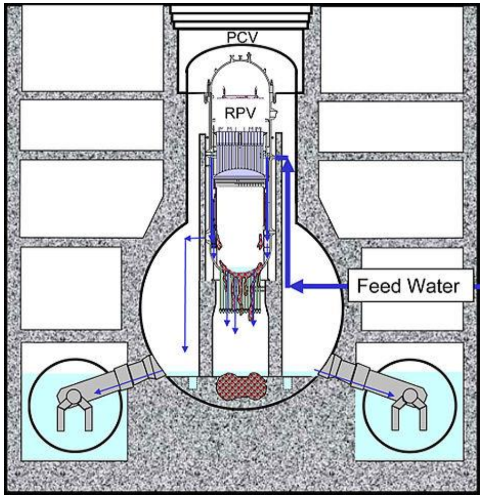
Fukushima Daiichi nuclear disaster



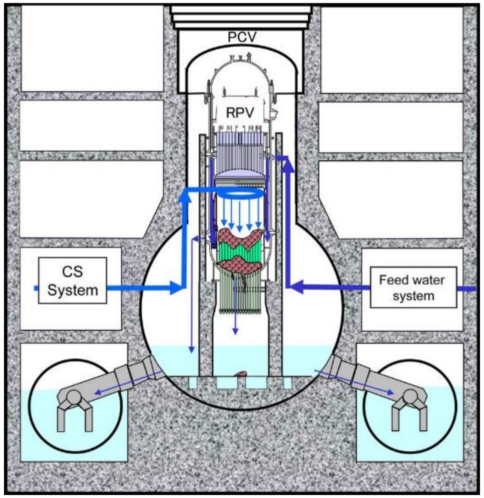
Fukushima Daiichi I nuclear power plant site close-up.



The height of the tsunami that struck the station approximately 50 minutes after the earthquake.



The suspected location of molten fuel inside Unit 1, according to the MAAP report from November 2011. Most of the fuel from Unit 1 is assumed to be at the bottom of the Primary Containment Vessel (PCV), where it is estimated to be "well cooled down".

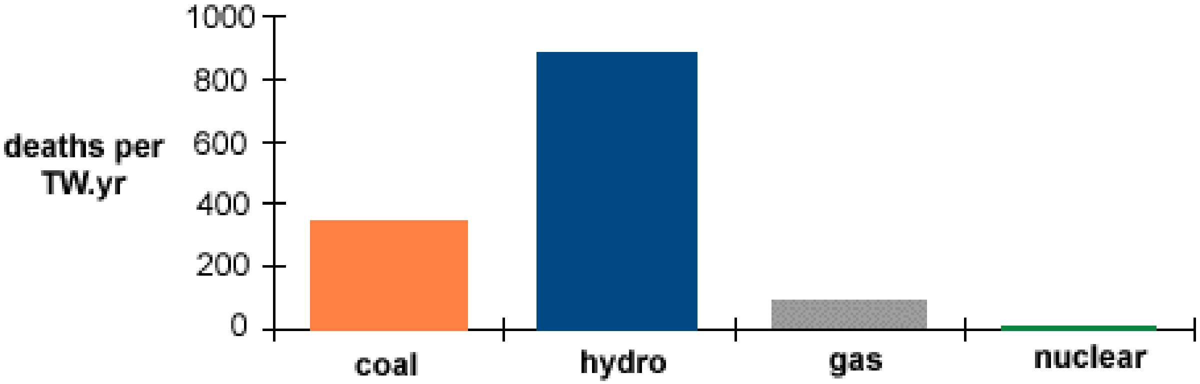


The suspected location of molten fuel inside Unit 2 and Unit 3, according to the MAAP report from November 2011. Most of the fuel from Units 2 and 3 was assumed to have remained in the Reactor Pressure Vessel (RPV).

Fukushima Daiichi nuclear disaster

Safety Relative to Other Energy Sources

Deaths from energy-related accidents per unit of electricity



Comparison of accident statistics in primary energy production

(Electricity generation accounts for about 40% of total primary energy)

Fuel	Immediate fatalities 1970-92	Who?	Normalized to 1/TWy* electricity
Coal	6400	workers	342
Natural gas	1200	workers & public	85
Hydro	4000	public	883
Nuclear	31	workers	8