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

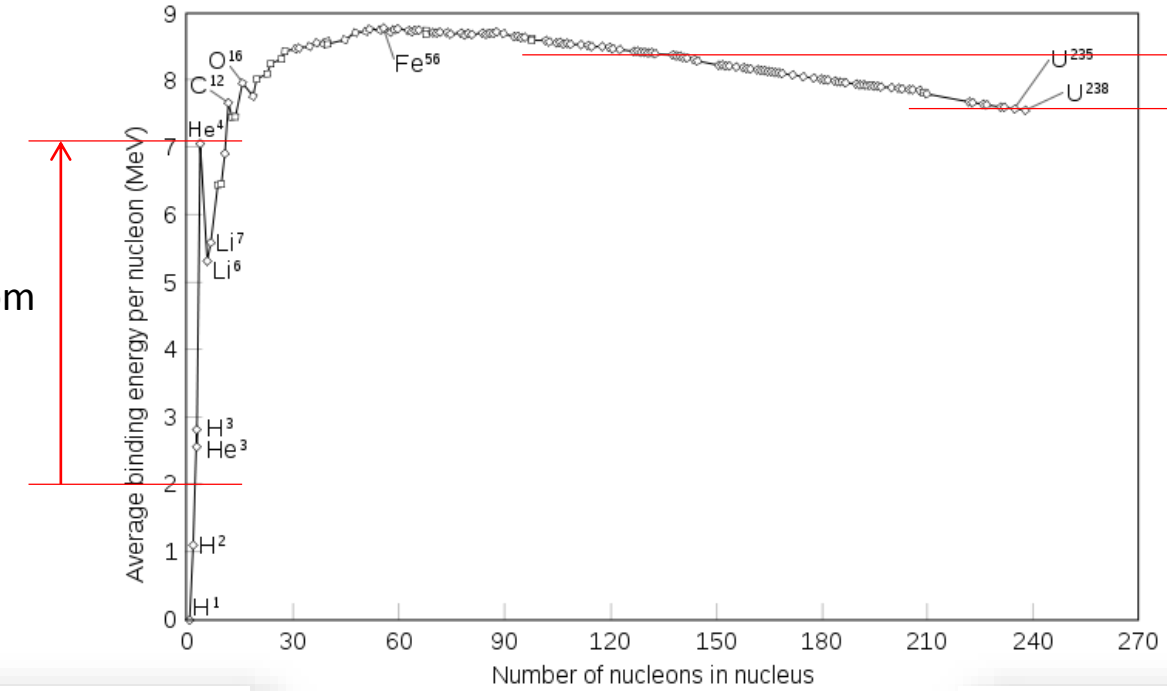
Introduction to Nuclear Energy and Nuclear Power Plants

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

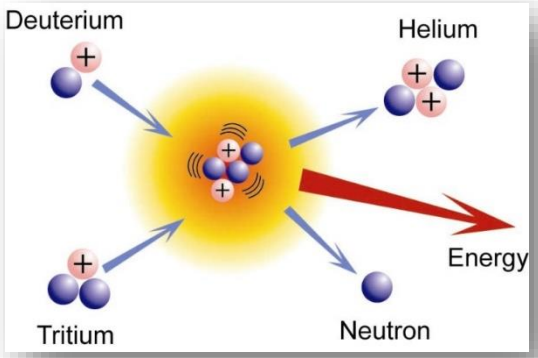
The Two Sources of Nuclear Energy Production

Energy yield from nuclear fusion

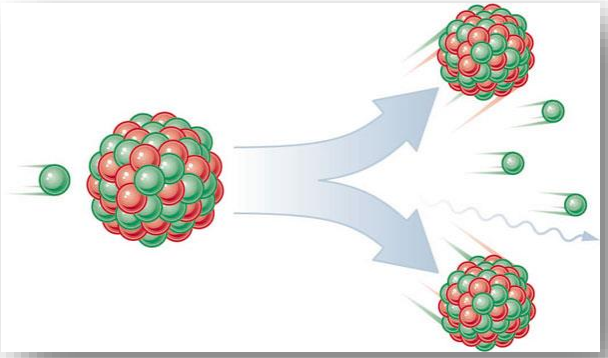


Energy yield from nuclear fission

Fusion



Fission

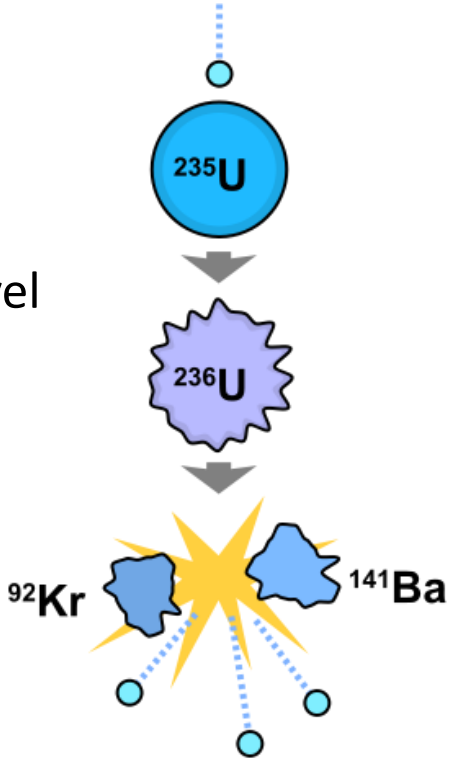


Comparison of Fission and Fusion

	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

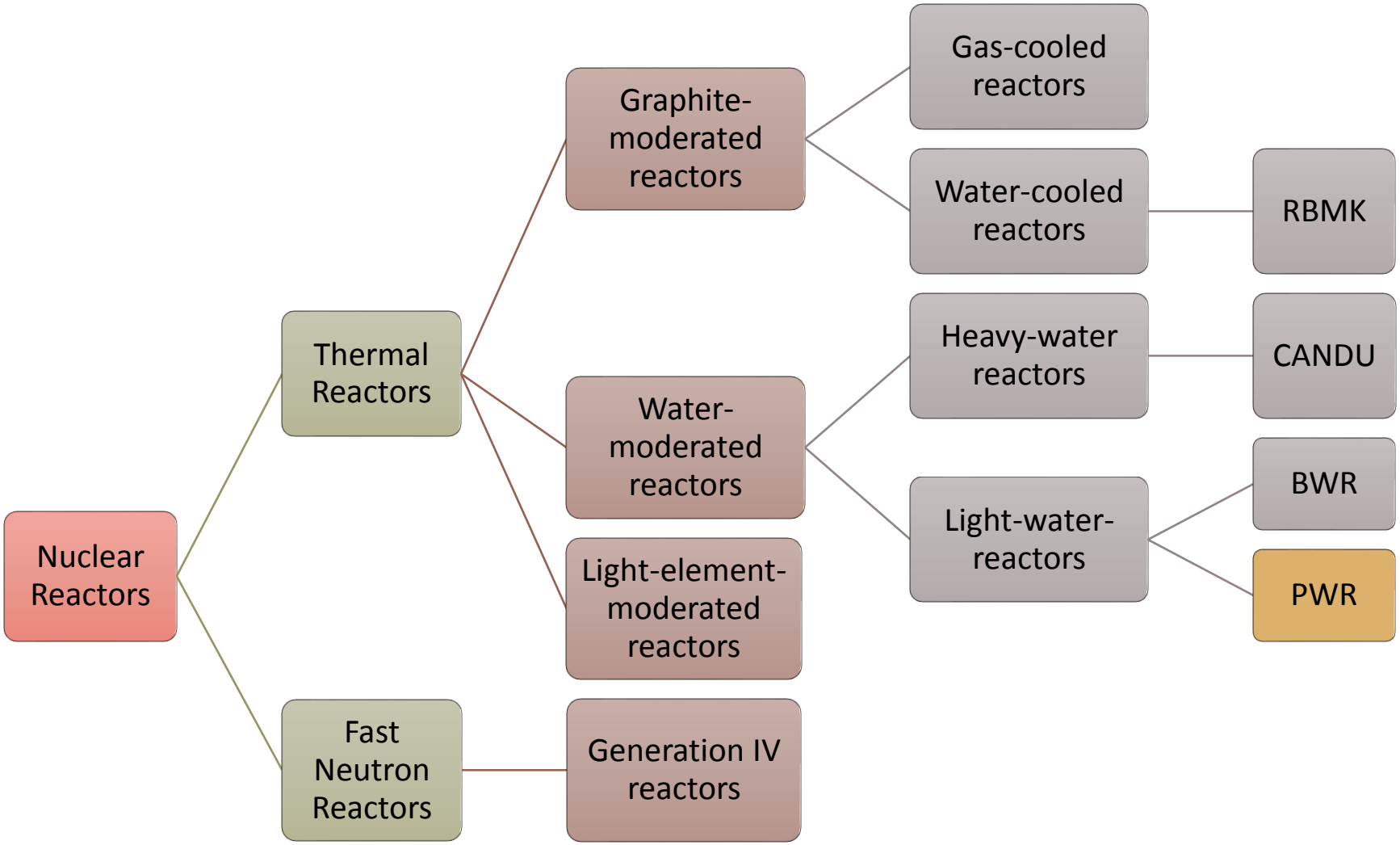
- Effective neutron multiplication factor (k) is the average number of neutrons from one fission to cause another fission
  - k < 1 (subcriticality): the system cannot sustain a chain reaction
  - k = 1 (criticality): every fission causes an average of one more fission, leading to a constant fission (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

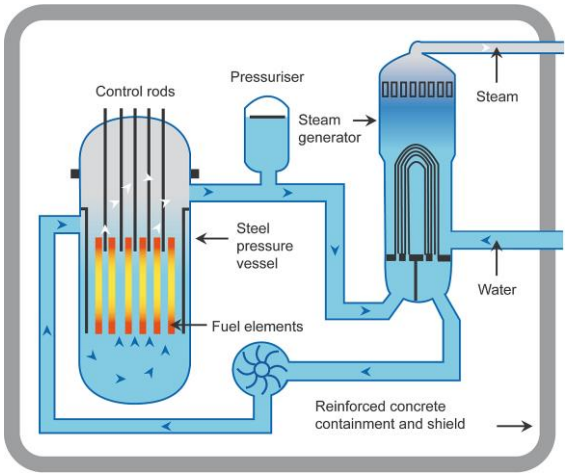
- Reactivity is an expression of the departure from criticality: $\rho = (k - 1)/k$
  - when the reactor is critical, $\rho = 0$
  - when the reactor is subcritical, $\rho < 0$
- The temperature coefficient (of reactivity) is a measure of the change in reactivity (resulting in a change in power) by a 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

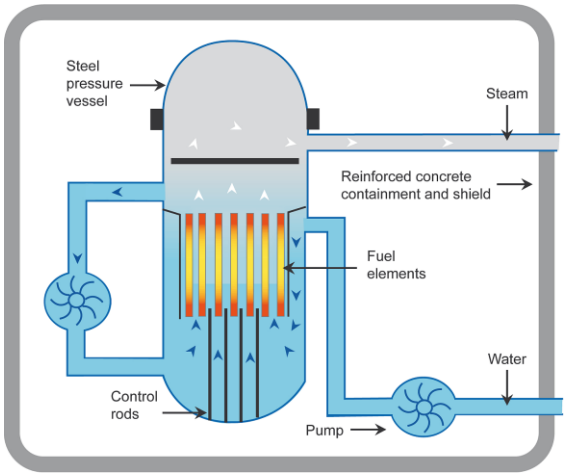


Typical Reactor Structures

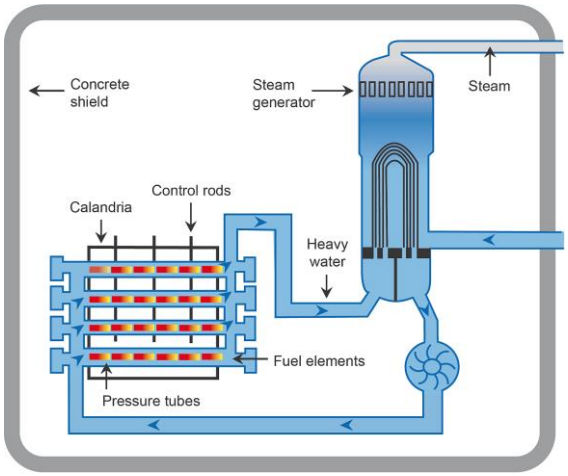
Typical Pressurized Light-Water Reactor (PWR)



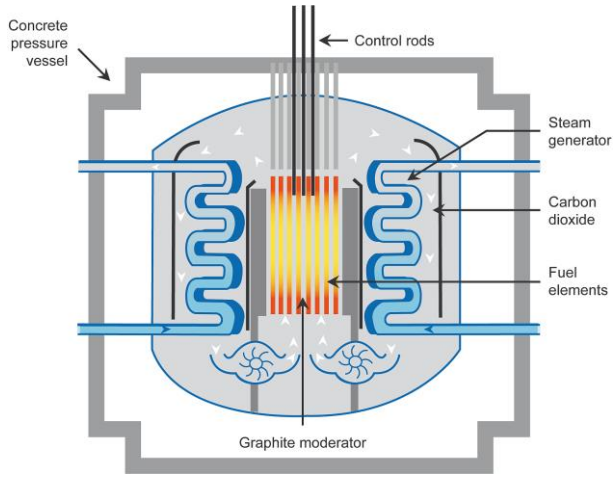
Typical Boiling Light-Water Reactor (BWR)



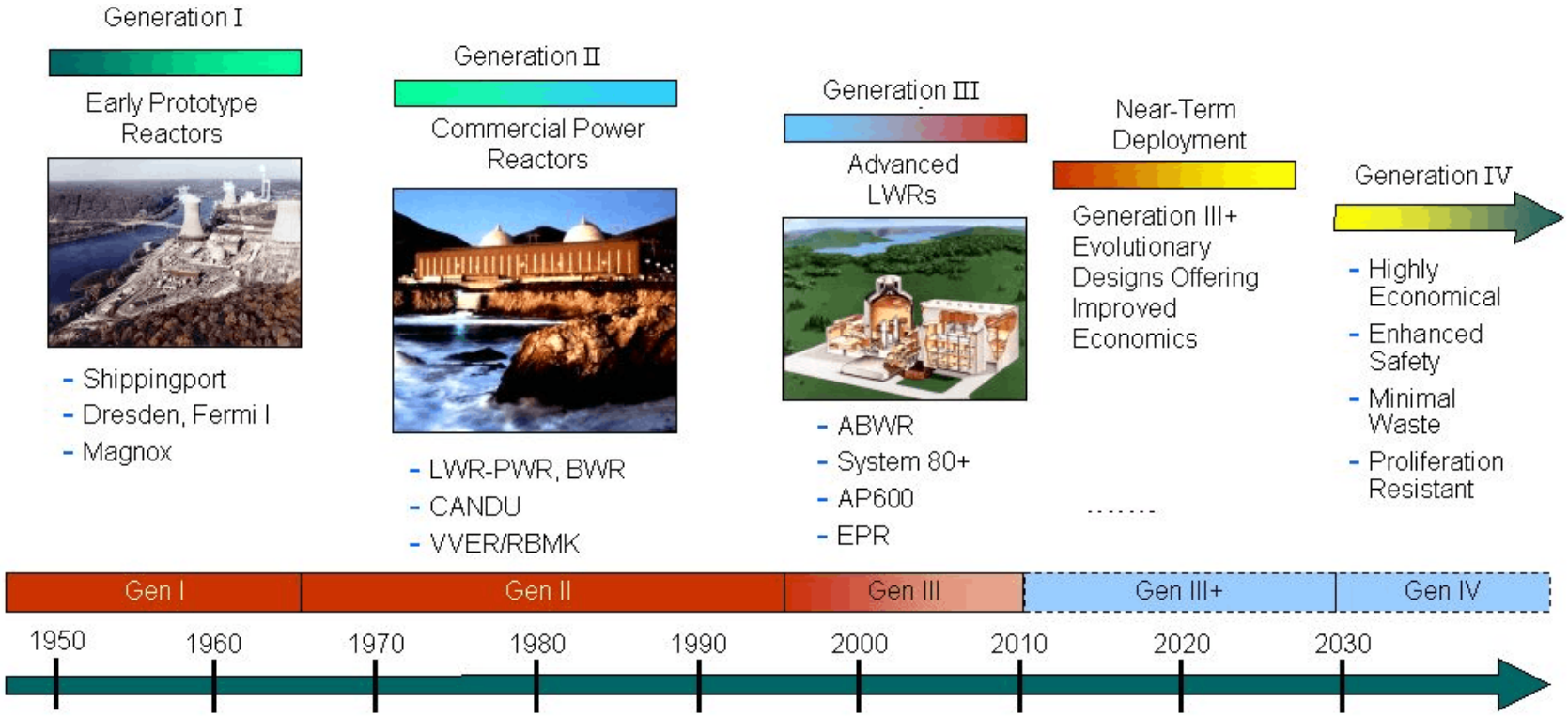
Typical Pressurized Heavy-Water Reactor (PHWR, CANDU)



Advanced Gas-Cooled Reactor (AGR)



Nuclear Reactor History and Generations



- Generation 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)

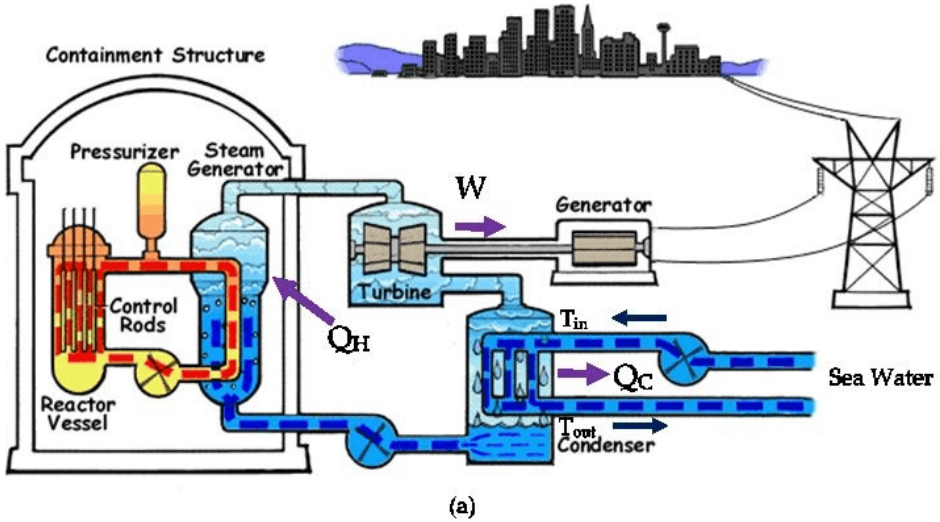
Heavy-water-cooled and -moderated pressurized-water reactors, fuel in tubes, efficient but expensive

High Power Channel Reactor (RBMK)

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

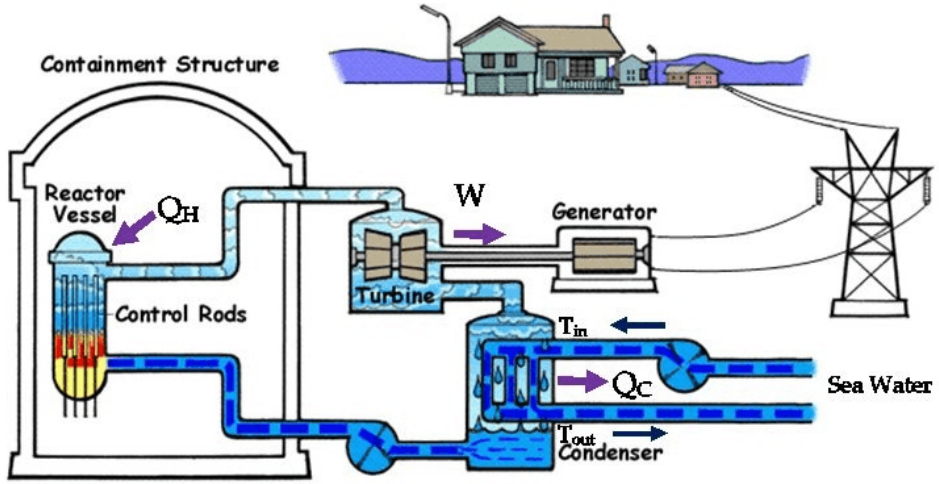
Common Light Water Moderated Reactors

Pressurized WR

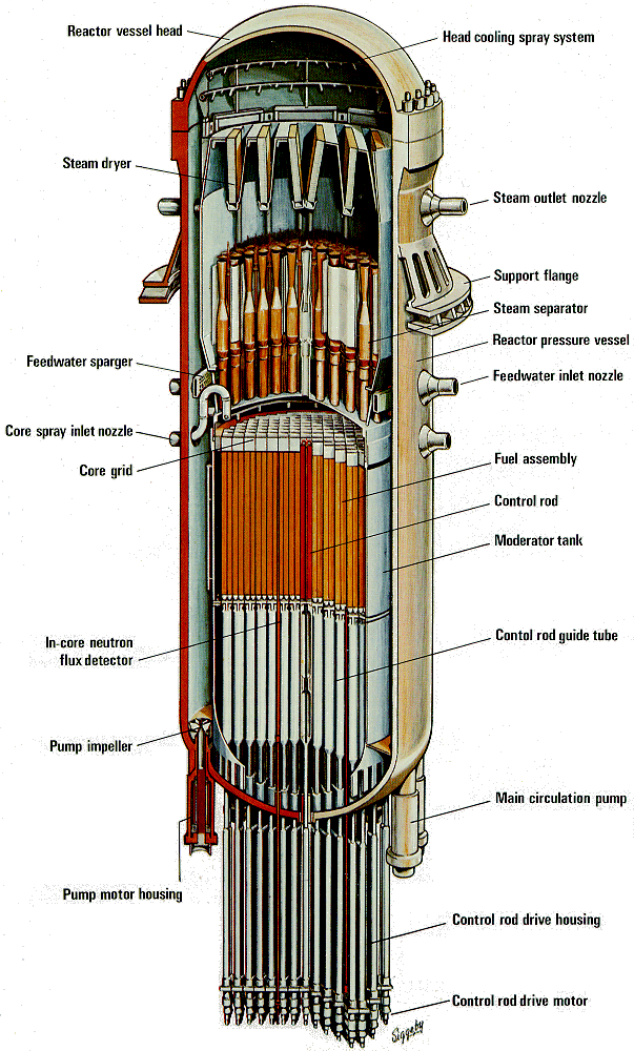


(a)

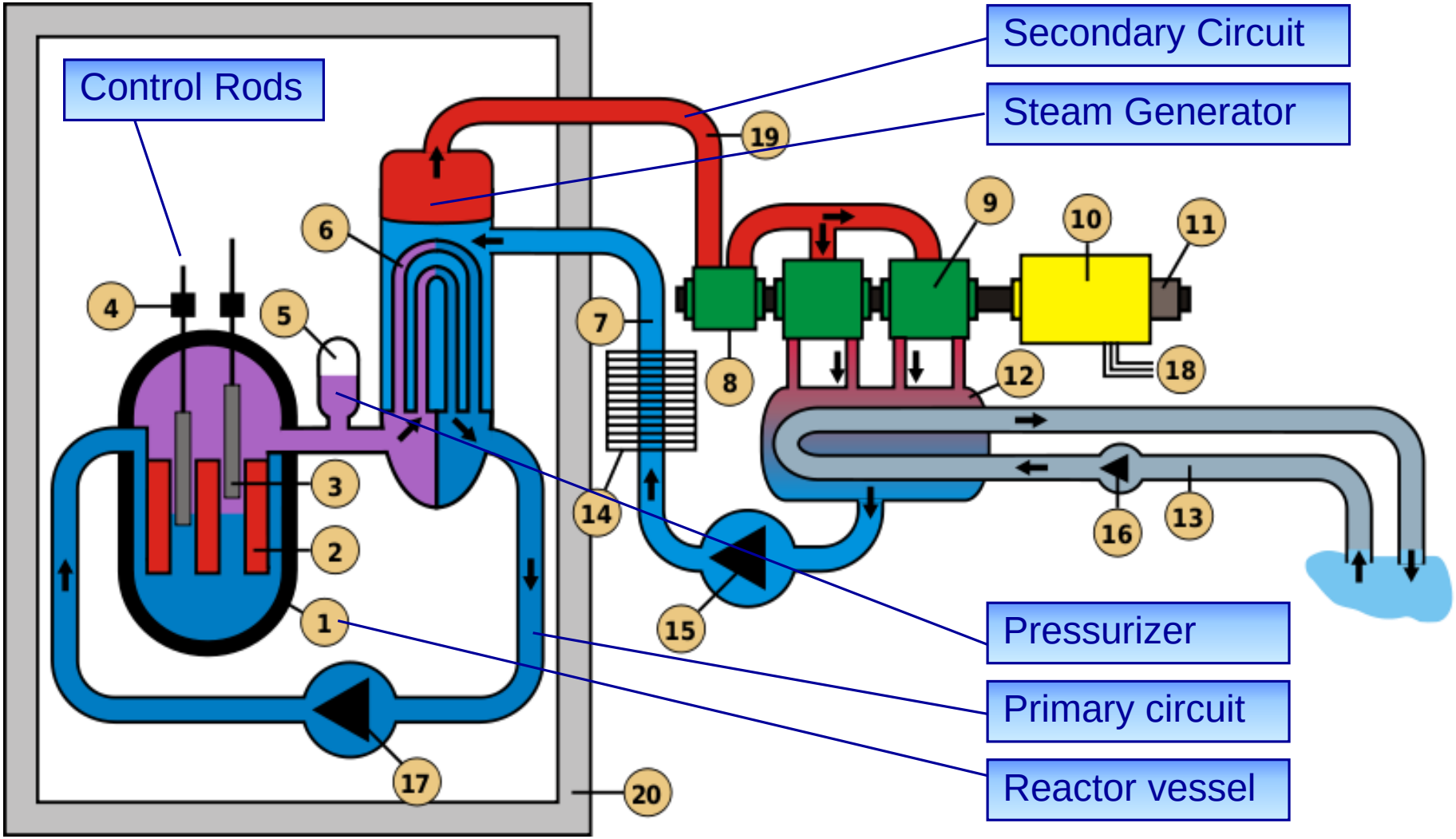
Boiling WR



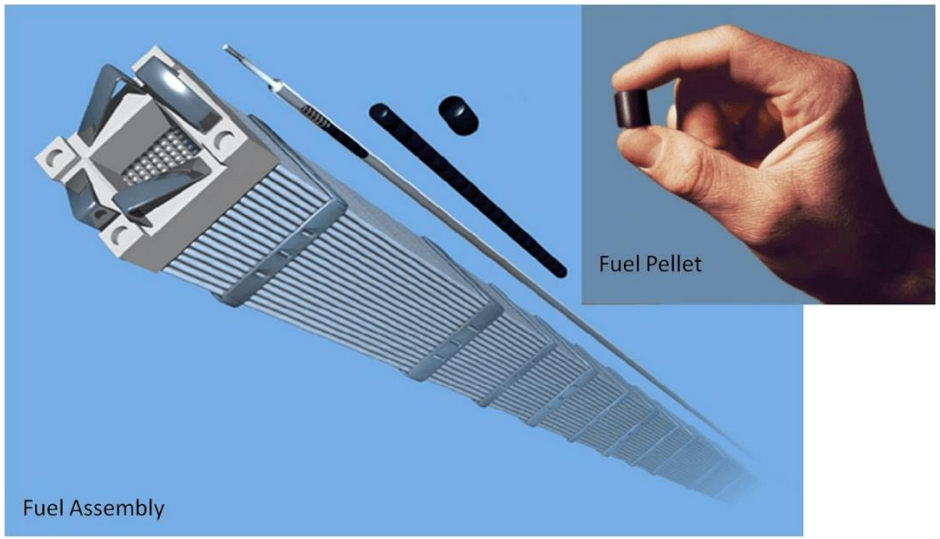
(b)

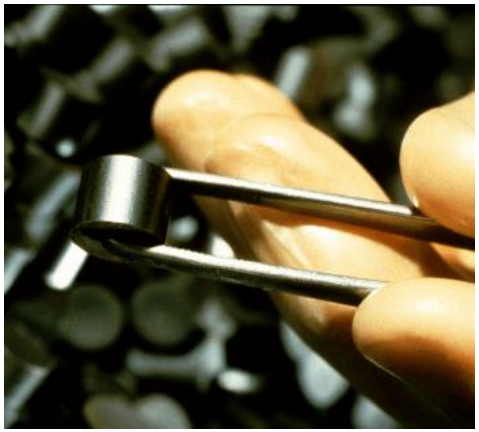


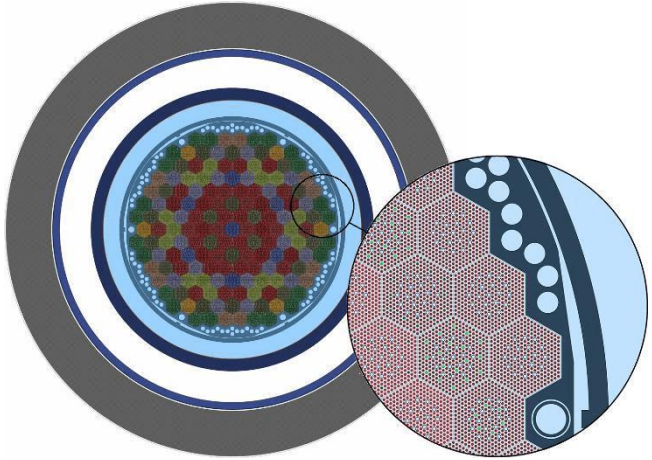
Overview of a PWR nuclear power plant



Fuel pellet and fuel assembly







Nuclear power in Hungary

Paks Nuclear Power Plant (Units 1–4, „Paks I.”)

- 4 VVER-440/213 model reactor units
- Nominal power ~2 GW electrical (since power uprate)
  - met 36.5% of domestic demand for electricity and
  - accounted for 51.3% of Hungary's national electricity output (2016)
- Capacity preservation started
  - units are/will be in their lifetime extension period
  - will have to be shut down between 2032 and 2037

Paks II. (Units 5–6)

- 2 MIR-1200 (AES-2006 V-491) model reactor units
  - Modernized International Reactor with 1.2 GW electrical
  - design life of 60 years
- Construction will start in 2020
  - the first unit is scheduled to be delivered in 2026 and
  - the second unit in 2027
- Not a turnkey project, customized to comply with Hungarian requirements

Risk of Nuclear Installations

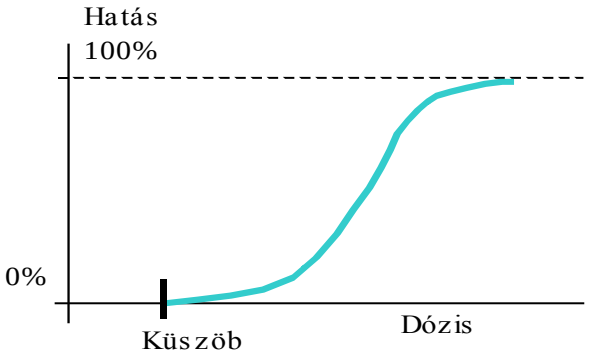
Using the Terms of the Functional Safety Concept

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

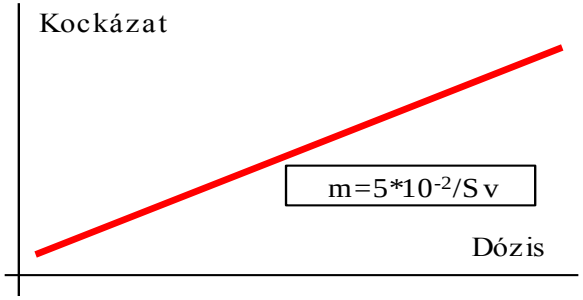
Consequence: Effects of Ionizing Radiation

Deterministic effect



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

Stochastic effect

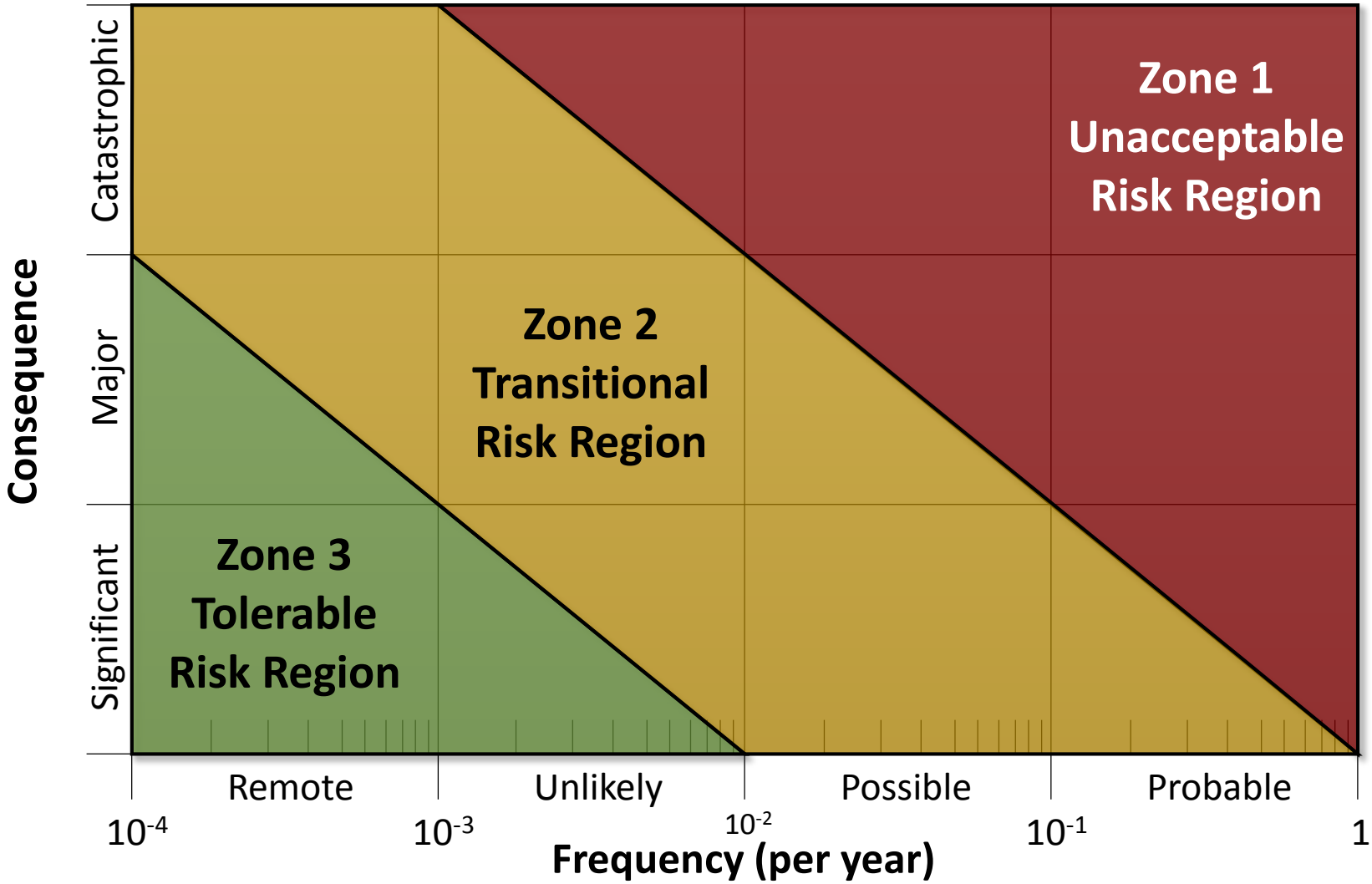


- Artificial radiation
  - Medical diagnosis and treatment
  - Industrial radiation sources
  - Nuclear tests
  - Nuclear waste

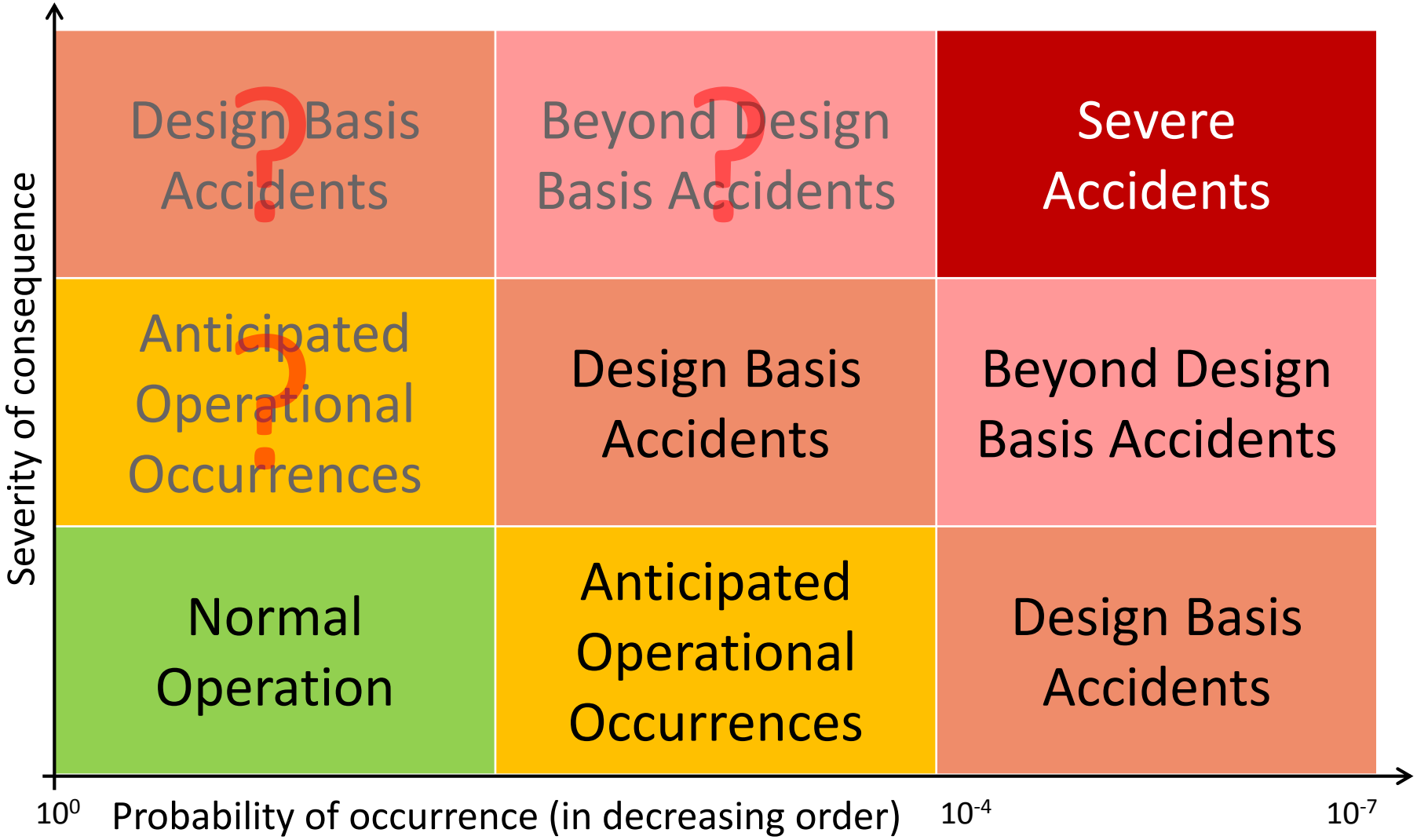
The Risk Assessment Framework

- 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



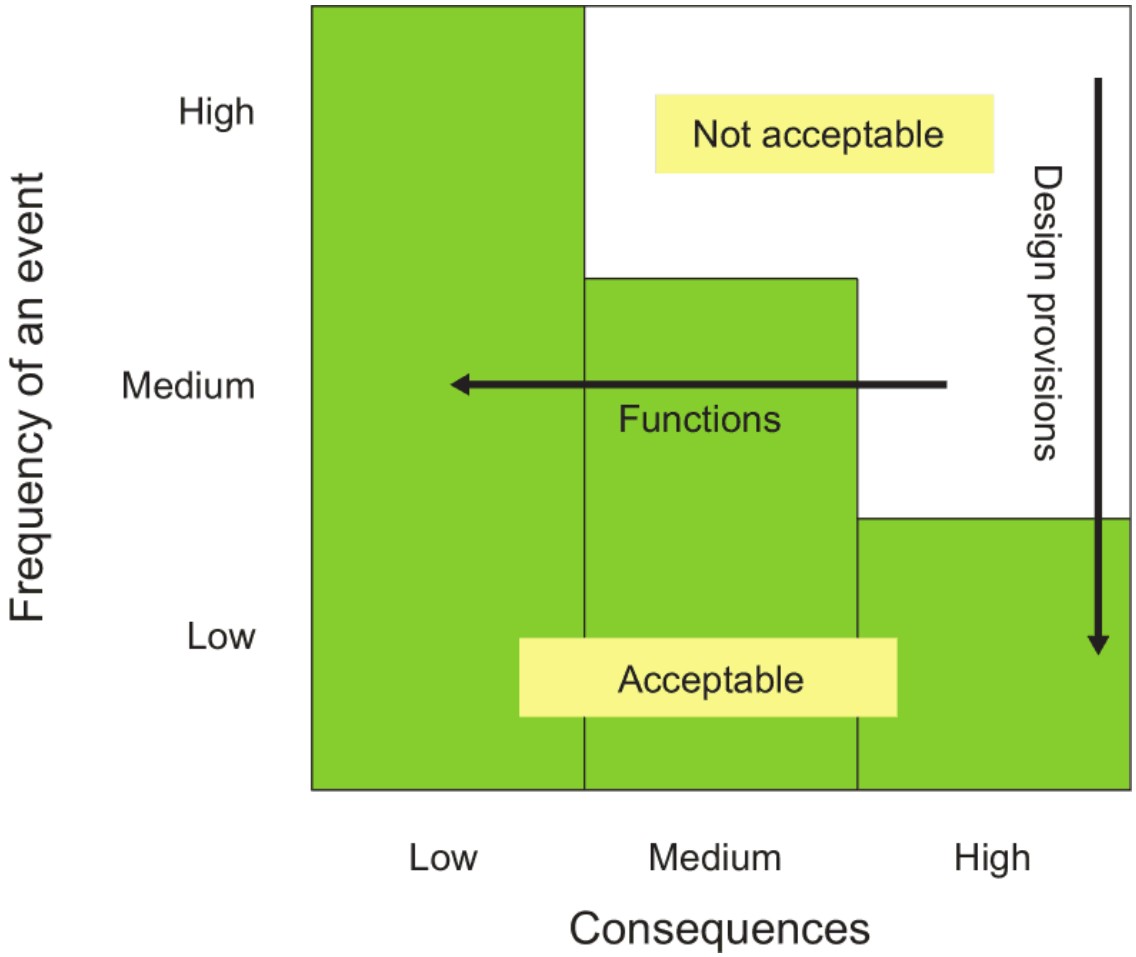
How would Risk Bands look like in Nuclear?



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

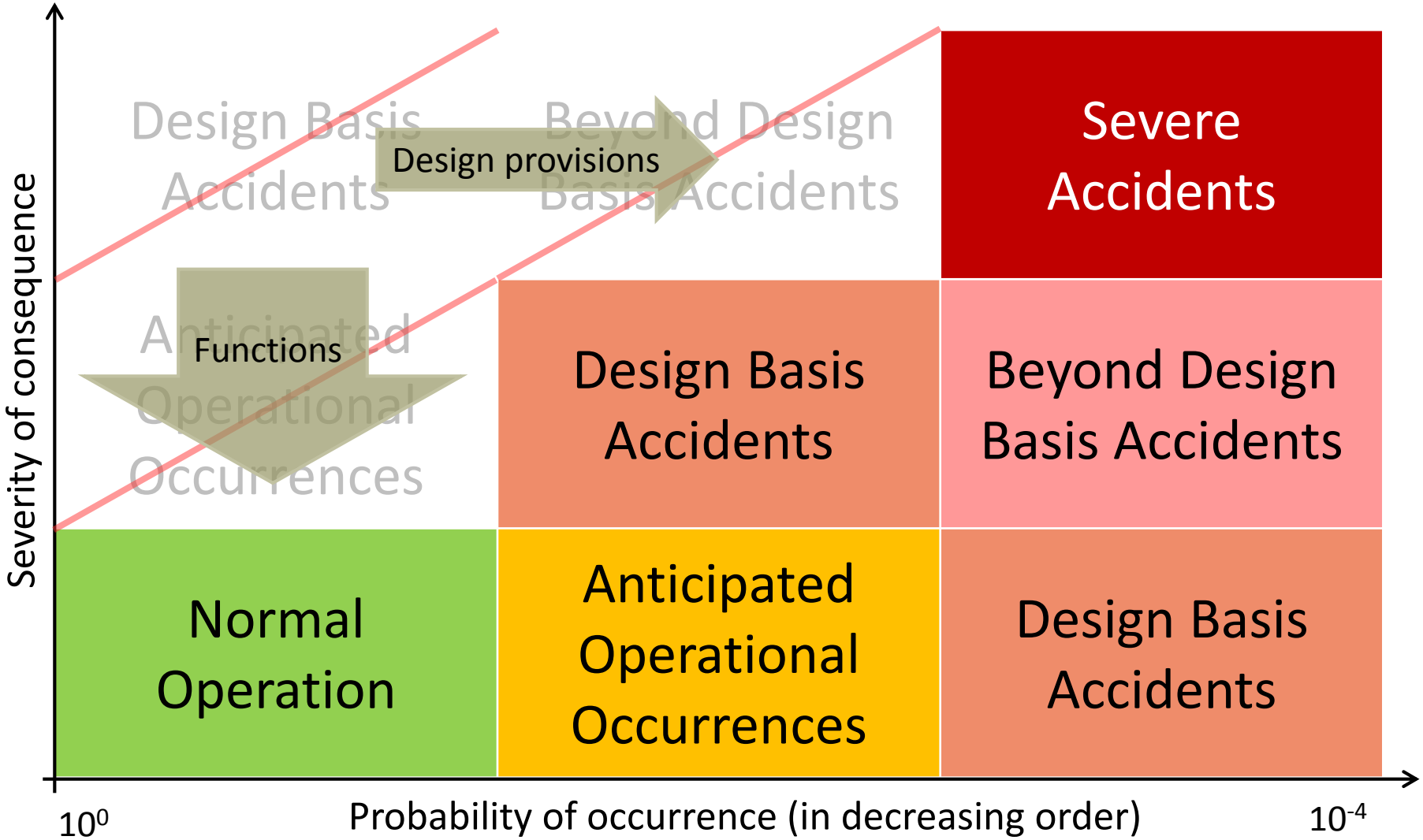
The Basic Principle of Frequency versus Consequences



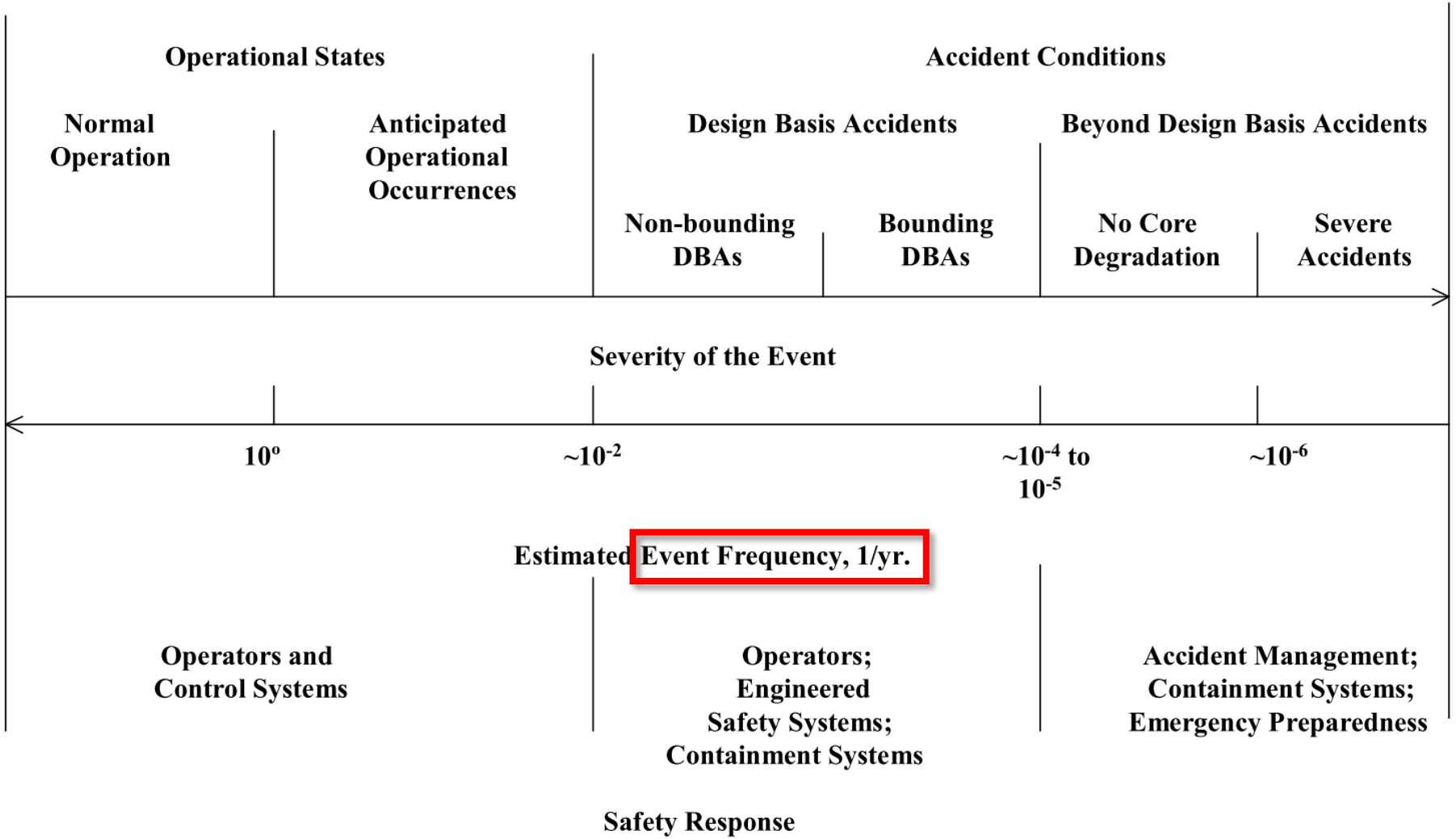
Design provisions are implemented primarily to decrease the probability of an accident, and functions are implemented to make the consequences acceptable with regard to their probability.

From the IAEA Specific Safety Guide No. SSG-30: Safety Classification of Structures, Systems and Components in Nuclear Power Plants

Thus, Risk Bands look in Nuclear like this:



Classification of Events & Operating Conditions

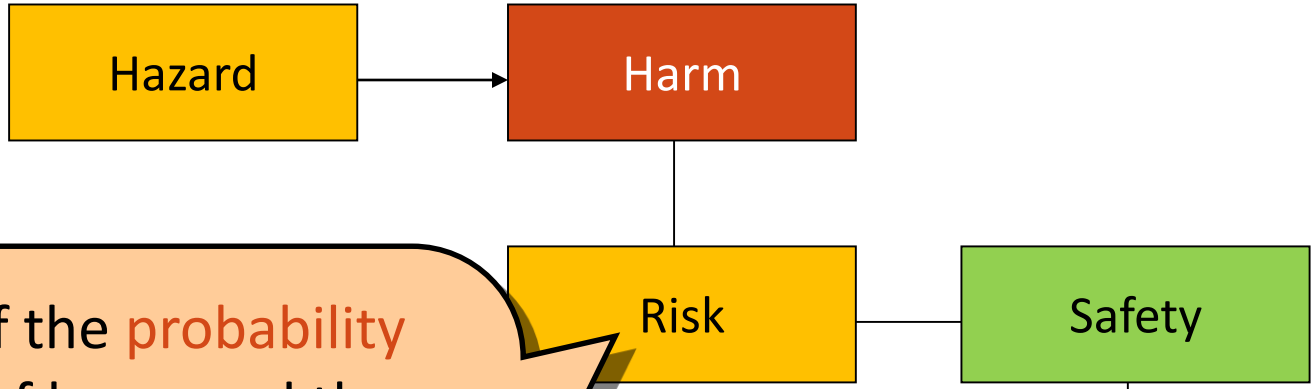


Plant states – according to IAEA SSR 2/1 / IEC 61226 / NSC

<table>
<tr><td colspan="2">Operational states</td><td colspan="4">Accident conditions (AC)</td></tr>
<tr><td colspan="6">IAEA SSR-2/1, IAEA SSG-30</td></tr>
<tr><td rowspan="2">Normal operation</td><td rowspan="2">Anticipated operational occurrences</td><td colspan="2" rowspan="2">Design basis accidents (DBA)
Design extension</td><td colspan="2">Design extension conditions (DEC)</td></tr>
<tr><td>–</td><td>Significant degradation of the reactor core</td></tr>
<tr><td colspan="6">IEC 61226 (Ed. 4 – Draft)</td></tr>
<tr><td rowspan="2">Normal operation</td><td colspan="3">Design basis event (DBE)</td><td colspan="2">Design extension conditions (DEC) …</td></tr>
<tr><td>Anticipated operational occurrences</td><td>– (AC not explicitly considered as design basis accident)</td><td>Design basis accidents (DBA)</td><td>w/o significant fuel degradation</td><td>with core melt</td></tr>
<tr><td colspan="6">NSC Volume 3. (operating units)</td></tr>
<tr><td rowspan="2">DBC1 (normal operation)</td><td colspan="3">Operational states considered as part of the design basis (DBC)</td><td colspan="2">Design extension conditions (DEC)</td></tr>
<tr><td>DBC2 (anticipated operational events)</td><td colspan="2">DBC4 (design basis incidents)</td><td>DEC1 (complex malfunctions without fuel melt)</td><td>DEC2 (serious accidents involving significant fuel melt)</td></tr>
</table>

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.

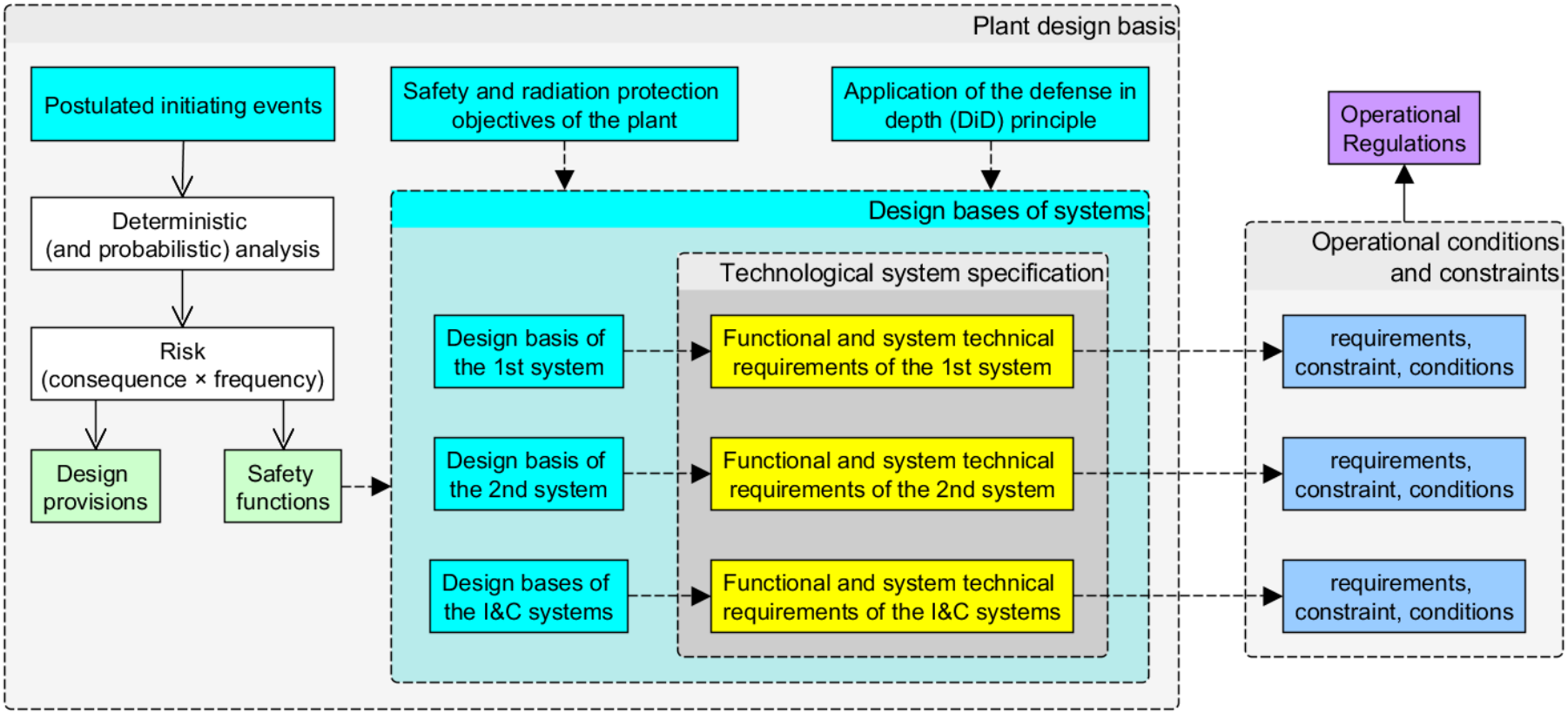
The Design Basis

- 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.

Fundamental safety functions and design basis

„Fundamental safety functions shall be achieved in the case of TA1-4 operating conditions. Following TAK1-2 operating conditions, the fundamental safety functions shall be performed to such a degree that the nuclear reactor can be brought to a controlled, safe shutdown condition, while following a severe accident to a safe condition. (NSC 3.2.1.0900)
„Systems shall be designed to perform the fundamental safety functions.” (NSC 3.2.1.1000)
„To perform the fundamental safety functions all safety functions and systems providing these safety functions shall be defined.” (NSC 3.2.1.1100)
„Monitoring of the status of the systems, structures and components of the nuclear power plant shall be provided in order to verify if the basic design requirements are fulfilled.” (NSC 3.2.1.1200)
„The criteria relating to the accuracy, response time, event sequence determination, processing capacity reserve and communication capacity reserve of the programmable instrumentation and control systems shall be specified consistent with the design basis of the nuclear power plant.” (NSC 3.4.5.2500.)

Connection between the plant and the I&C system design bases



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

Requirements for I&C systems are based on a Graded Approach

Graded approach (specifying differentiated requirements):

- The relevance to nuclear safety of nuclear I&C systems imposes high reliability on many I&C functions.
- Reliability is achieved through progressive application of the required design principles:
  - Achieving a high level of functional reliability is both labor-intensive and costly; therefore, resources must be focused on elements that have the highest influence on increasing security.
  - For this, the design principles are increasingly strict in correspondence to the safety importance of the functions, subsystems and components of the I&C system.
- The first step in this graded approach is to categorize I&C functions into safety categories according to their relevance to safety.
- I&C systems that perform the safety-relevant I&C functions are categorized into safety classes based on the highest safety category function they perform.
- Both the function safety categories and the equipment safety classes can (and usually do) have associated requirements.

„The design and implementation of the instrumentation and control systems and system components shall be carried out in accordance with the selected standards applicable to systems and system components of the relevant safety class and differentiated requirements.” (NSC 3.4.5.2000.)

NSC 3a. Safety level of plant safety functions

Operating state	Description	Event frequency (f [1/y])
DBC1	Normal operation	-
DBC2	Anticipated operational occurrences	$f \geq 10^{-2}$
DBC3	Infrequent design basis accidents	$10^{-2} > f \geq 10^{-4}$
DBC4	Rare design basis accidents	$10^{-4} > f \geq 10^{-6}$

a) F1A level to the safety functions that are required to bring DBC2-4 operating states to a controlled state;

b) F1B level to the safety functions that
- ba) are required to bring the nuclear power plant unit from DBC2-4 operating states to a safe shutdown state and keep it in a safe shutdown state for at least 24 hours,
- bb) replace the F1A functions following their failure, and help to keep the BDB operating states in the DEC1 operating state,
- bc) all normal operating functions, the loss of which may result directly in TA3-4 operating states.

c) F2 level to the safety functions that
- ca) are required after 24 hours following the DBC2-4 operating states to keep the nuclear power plant unit for at least 72 more hours in a safe shutdown state,
- cb) the safety functions taken into consideration in the extension of the design basis,
- cc) are designed to prevent malfunctions not related to the active zone of the nuclear reactor, and
- cd) all normal operating functions, the loss of which may cause DBC2 operating state and directly initiate reactor protection function activation.

Nuclear Accidents

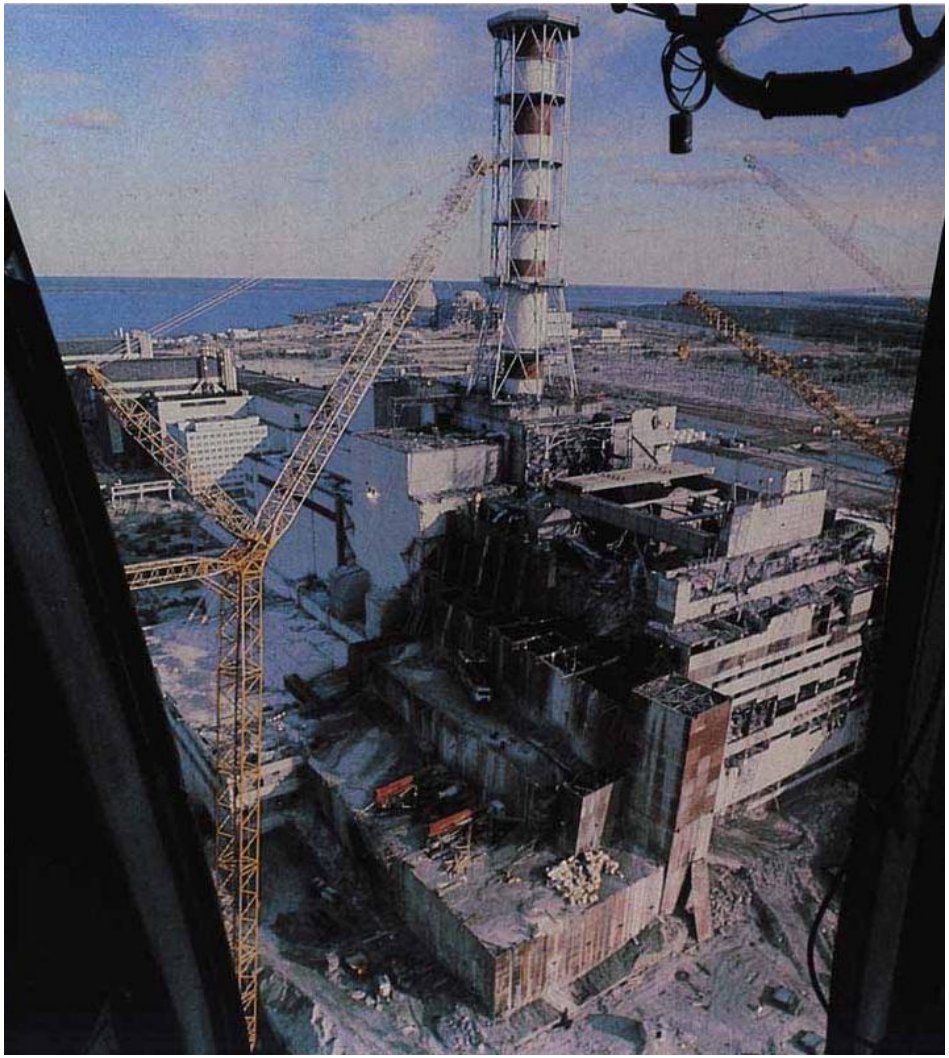
The Three Most Prominent Accidents in the History of Nuclear Power Generation, and Lessons Learned

Main Types of Nuclear Reactor Accidents

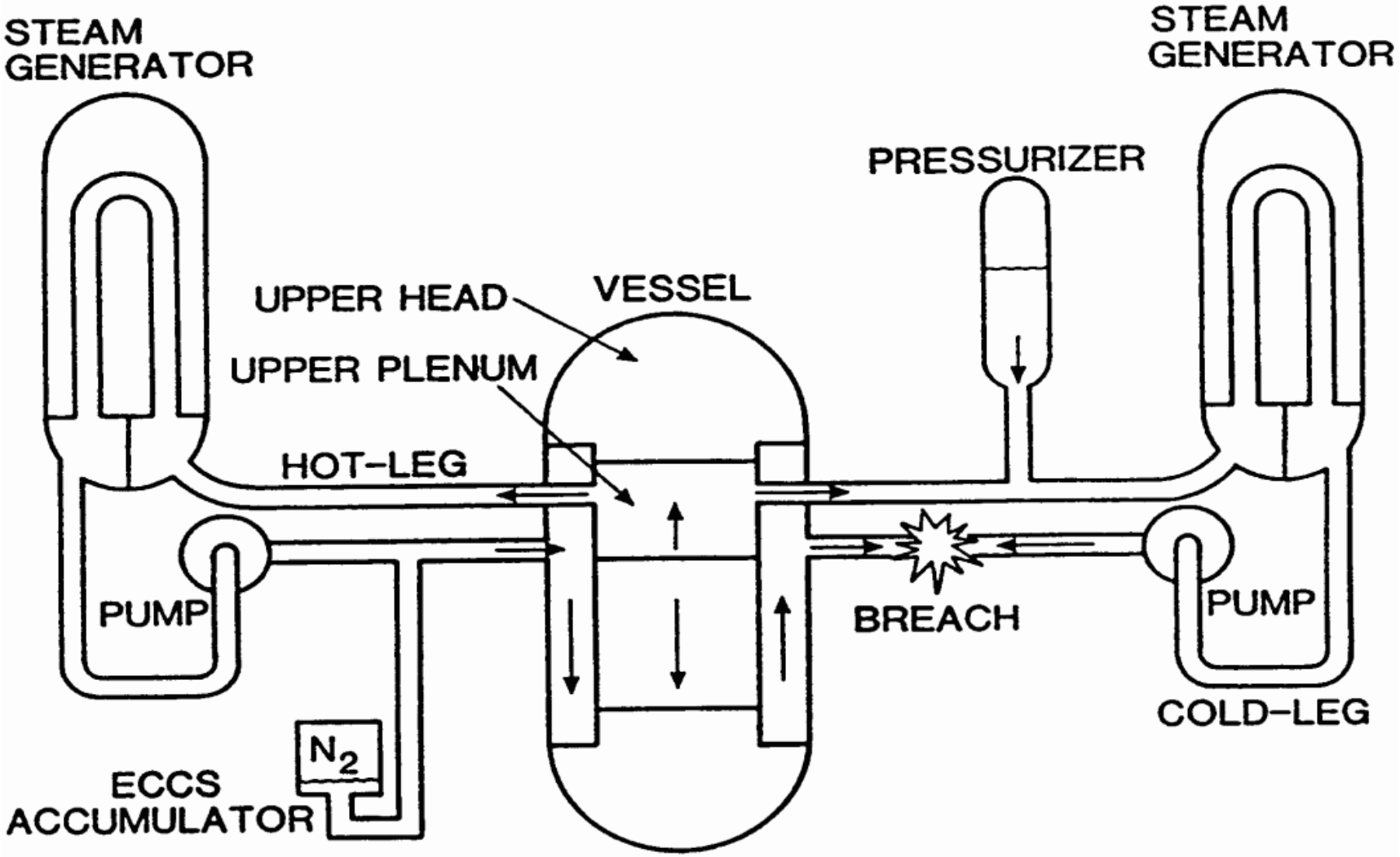
- Accident initiated by sudden reactivity increase (e.g. control rod ejection) that causes reactor runaway
  - RIA – Reactivity Initiated Accident
  - the nuclear chain reaction becomes uncontrollable
    - prompt supercritical reactor
- Accident initiated by insufficient cooling (e.g. due to loss of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

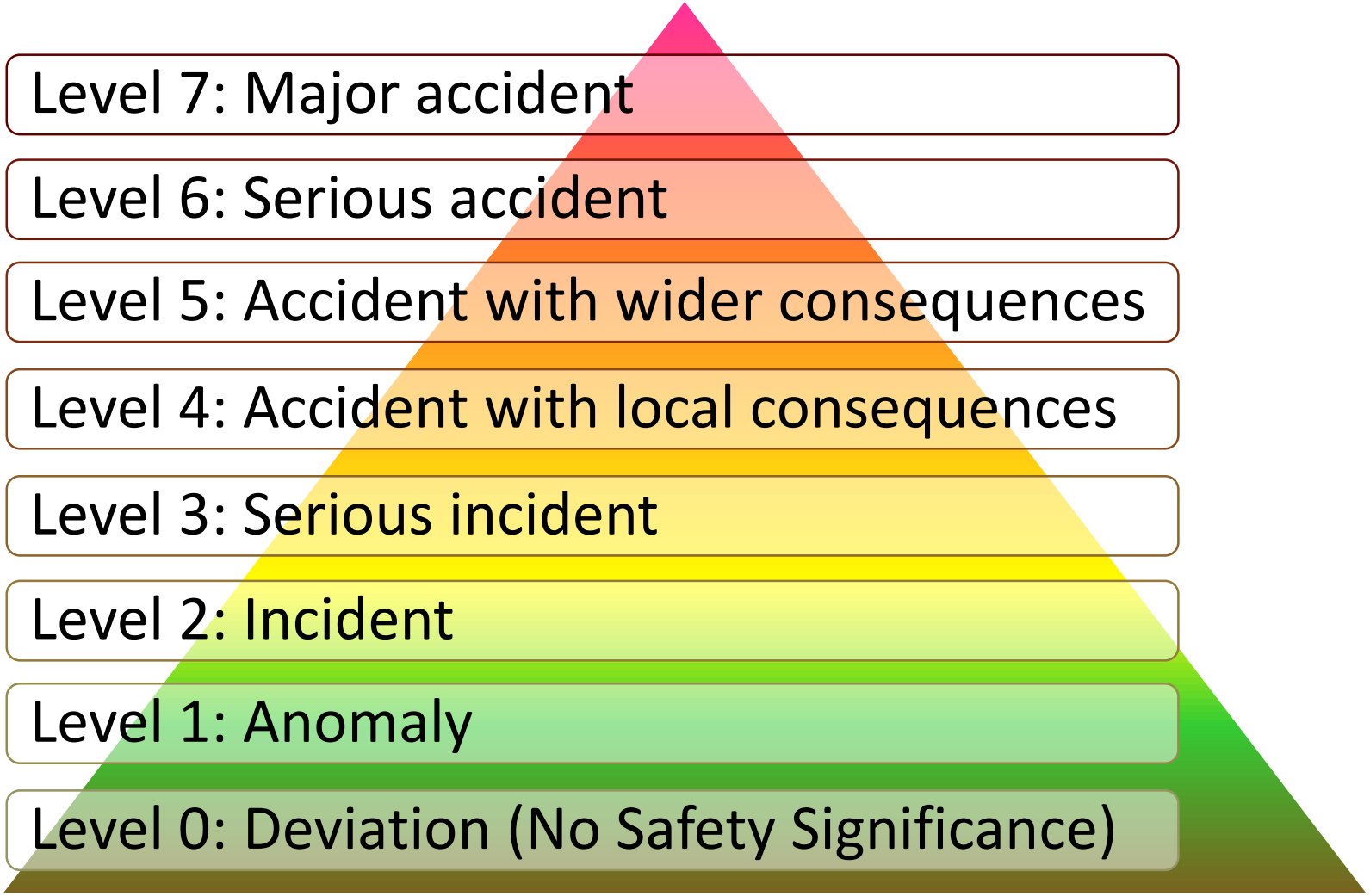
Reactivity Initiated Accident



Loss of Coolant Accident – LB LOCA

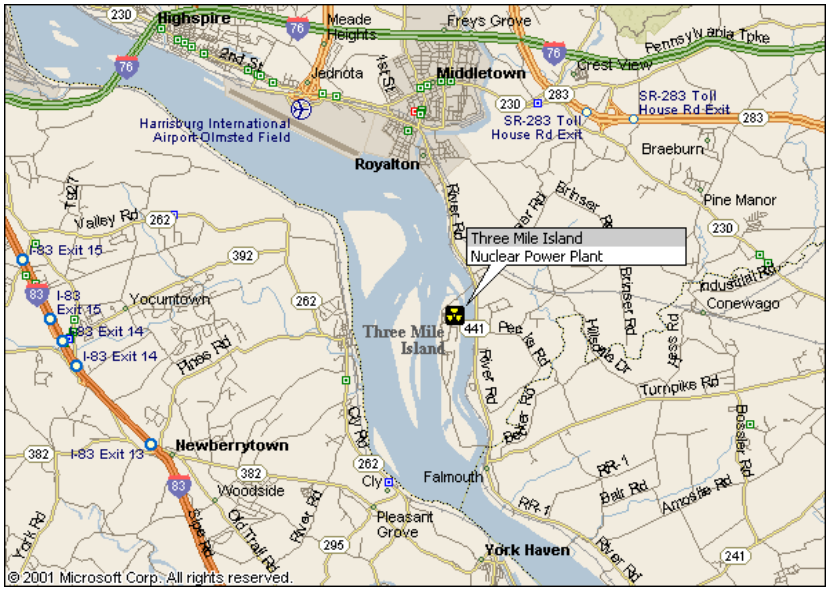


International Nuclear Event Scale (INES)



Details and Examples of the INES Scale

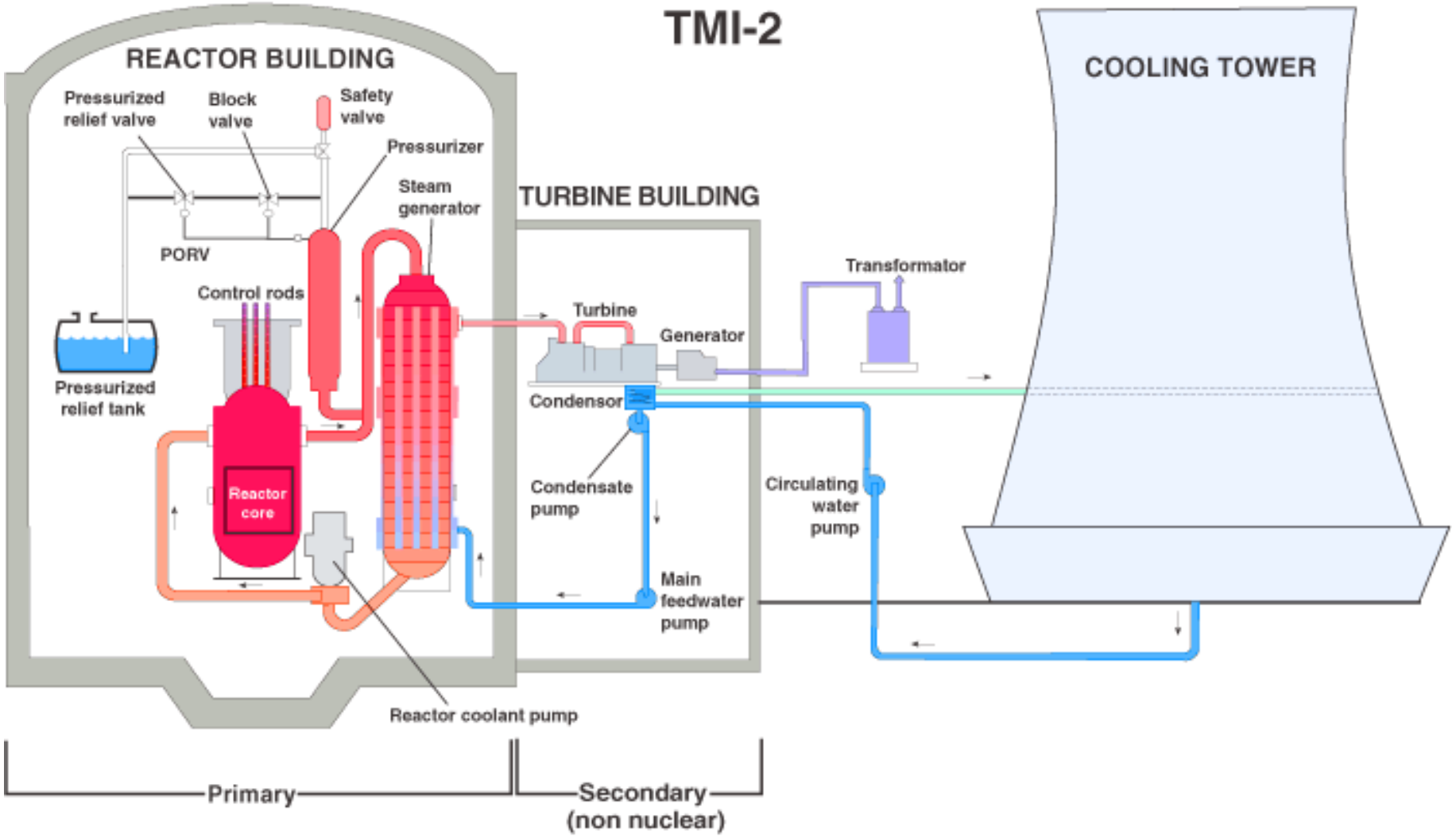
INES Level	People and Environment	Radiological Barriers and Control	Example
Level 7: Major accident	Major release of radioactive material Widespread effects		Chernobyl accident (Soviet Union), 26 April 1986 Fukushima accident
Level 6: Serious accident	Significant release of radioactive material		Kyshtym 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. The TMI-2 reactor was destroyed.
- Some radioactive gas was released a couple of days after the accident, but not enough to cause any dose above background levels to local residents.
- There were no injuries or adverse health effects from the Three Mile Island accident.

Three Mile Island Accident

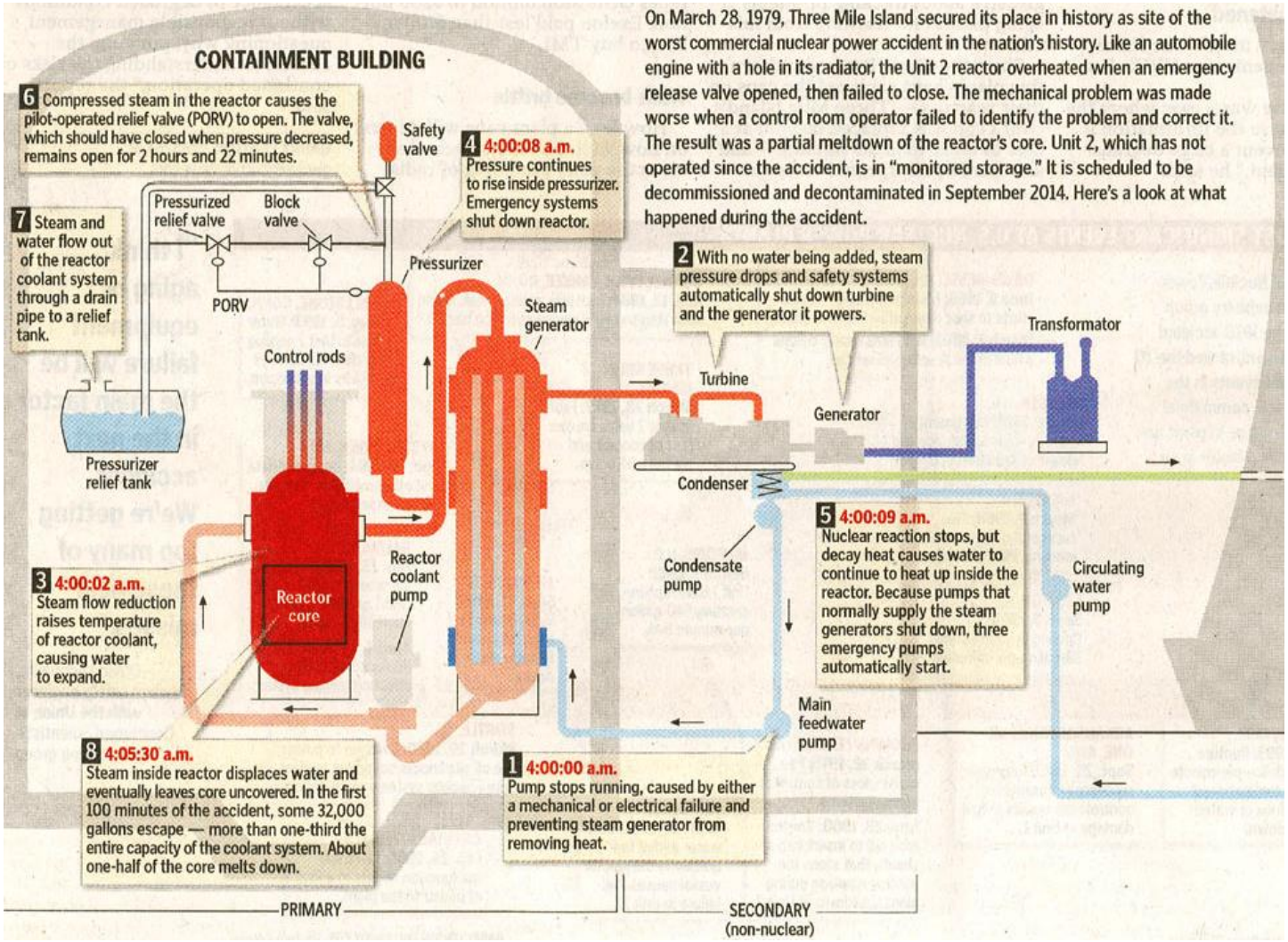


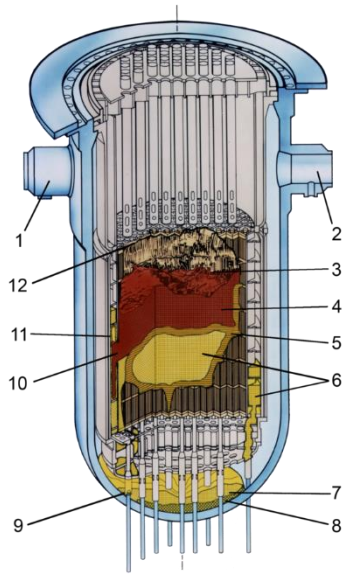
Three Mile Island Accident

- 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

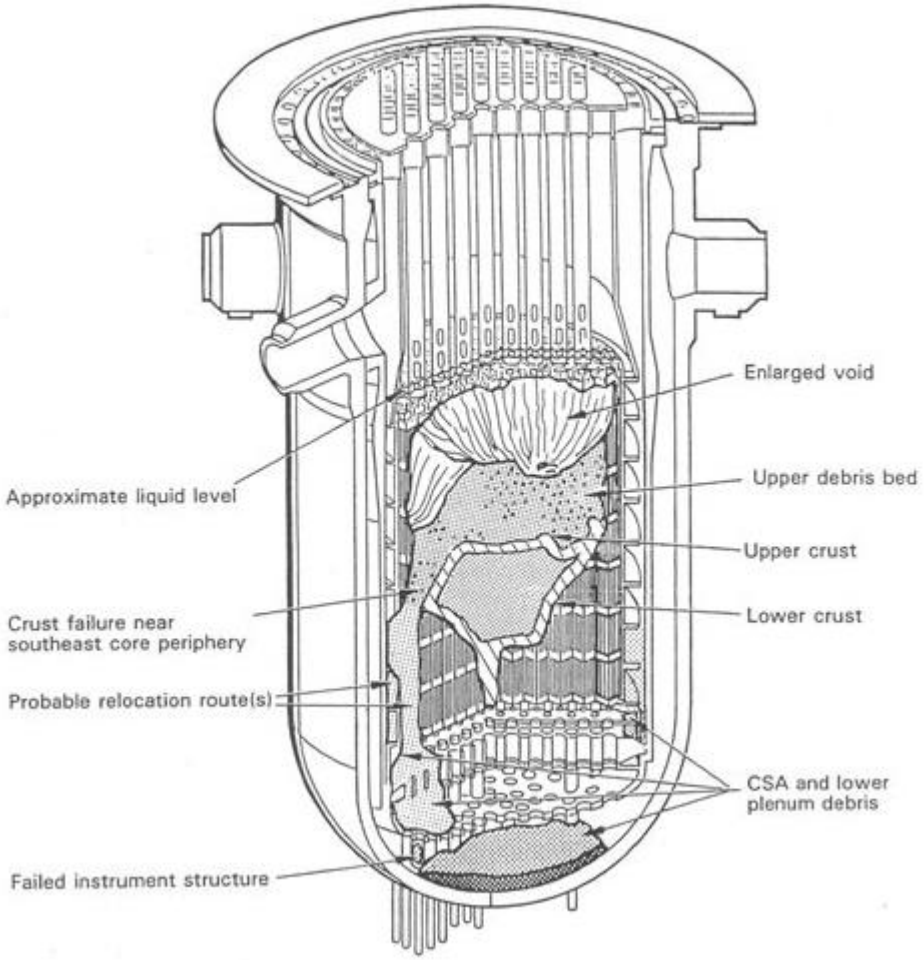
On March 28, 1979, Three Mile Island secured its place in history as site of the worst commercial nuclear power accident in the nation's history. Like an automobile engine with a hole in its radiator, the Unit 2 reactor overheated when an emergency release valve opened, then failed to close. The mechanical 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.

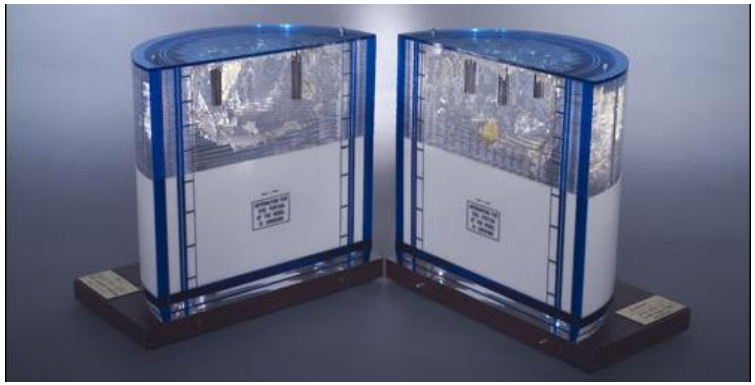


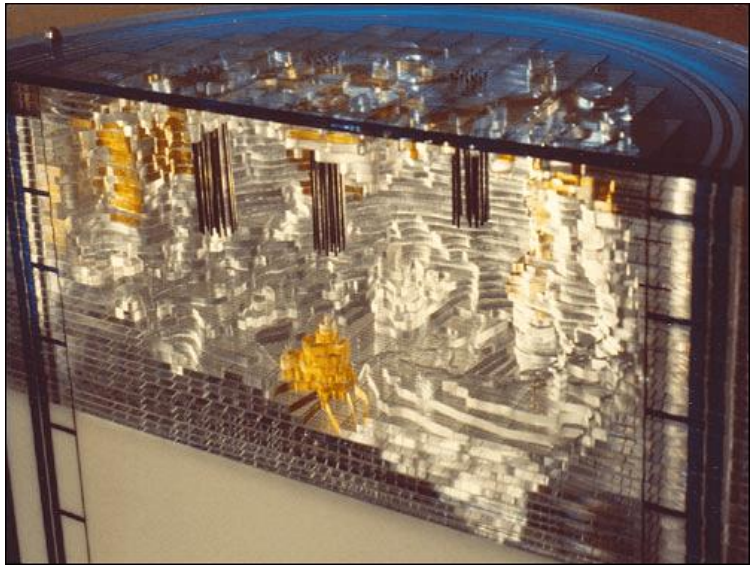


NRC graphic of TMI-2 core end-state configuration

TMI-2 reactor vessel after the accident







Lessons learned: example requirements

3a.4.4.0200. **Sufficient display, archiving and actuating devices** shall be available for the operating personnel in the unit main control room for TA1-4, TAK1 and TAK2 operating conditions for the following purposes:

a) appropriate **monitoring of the condition** of the nuclear power plant unit and its **systems, structures and components**,

b) clear and timely indication of **any changes with a significant effect on safety**,

c) identification of **any automatic protective operation** and if not actuated, **their subsequent actuation**, and

d) **development of an overall picture of the processes** of the nuclear power plant unit.

Lessons learned: example requirements

3a.4.4.1400. The following requirements shall be taken into account during the design of the unit main and backup control rooms:

a) **stable and balanced division of tasks** and **sufficient information devices** shall be provided for the operating personnel,

b) the logical functional classification of the displayed information and the actuating devices shall be provided, with **special regard to ensuring** that the classification of information and interventions **is not contradictory**, and

c) it shall be ensured that **no unnecessary or insignificant information is displayed**.

3a.4.4.1500. The following requirements shall be taken into account during the design of the unit main control room:

a) **option for the screen-based monitoring** of systems and processes and high-capacity computer technology devices **supporting the operating personnel** shall be provided,

b) the **unified overview of the actual condition and main parameters** of the nuclear power plant unit shall be ensured in a **clearly visible and easily interpretable manner** for the unit main control room personnel, and

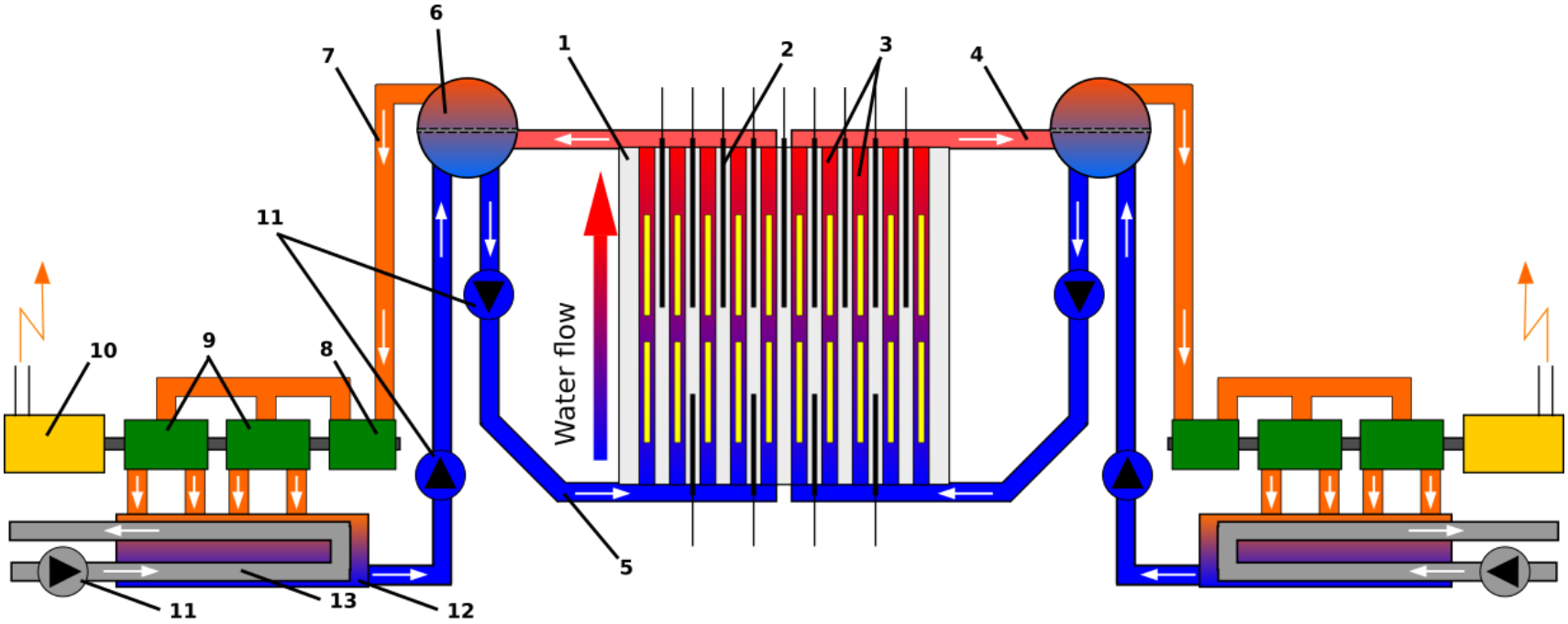
c) …

Chernobyl Accident

- The Chernobyl accident in 1986 was the result of a flawed reactor design that was operated with inadequately trained personnel.
- The resulting steam explosion and fires released at least 5% of the radioactive reactor core into the atmosphere and downwind – some 5200 PBq (I-131 eq).
- 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.

Chernobyl Accident

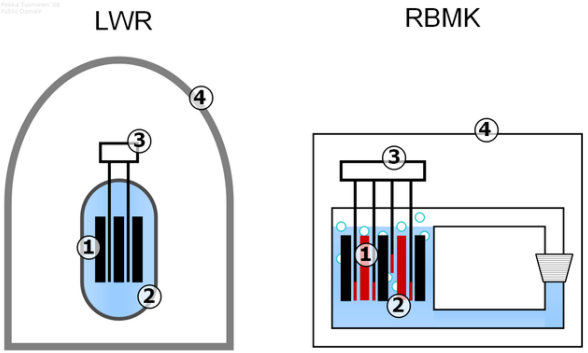
Schematic diagram of the RBMK reactor



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

- 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 has a positive void coefficient due to deficiencies in the design
  - 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

Lessons learned: example requirements

3a.3.1.1600. The appropriate design of the system performing the automatic shutdown of the nuclear reactor and controlling the systems providing active safety functions **shall ensure that** in the case of events resulting in either TA1 or TA2-4 operating conditions, **the operating personnel cannot prevent automatic safety actuation** from their established operating control positions, **while being able to perform the necessary interventions**.

Lessons learned: example requirements

3a.4.1.1200. The shutdown of the nuclear reactor and the control of its reactivity shall be ensured by **at least two systems** that **operate according to different principles** and provide an F1A safety function, of which **at least one shall be able by itself to shut down** the nuclear reactor from TA1-4 operating conditions. **At least one** of the shutdown systems **shall be automatic** and **quick-actuation**, which, if the pre-determined conditions are met, shuts down the nuclear reactor with high reliability **in an uninterrupted manner regardless of the activities of the operating personnel**. The reactor protection system generating the protection signal giving an instruction for a quick shutdown of the reactor shall also perform its task **even if one of the branches of the system fails** and, simultaneously, **another branch is also inoperable due to maintenance** or testing. In addition, both shutdown and control systems shall be single failure tolerant, even in the case of failure of any electric power supply or the **inoperability of the control rod assembly of the highest worth**.

Lessons learned: example requirements

3a.4.1.1500. It shall be ensured by the appropriate design of the systems controlling reactivity and shutting down the nuclear reactor that in TA1-4 operating conditions, **it is excluded that the safety limits** applicable to the temperature of the nuclear fuel and coolant and to other physical parameters **are exceeded**.

3a.4.1.1600. The **power coefficient of reactivity of the active core shall remain negative** in TA1-4 and TAK1 operating conditions.

3a.4.1.1700. The systems controlling reactivity and shutting down the nuclear reactor shall be so designed that **the extent and rate of reactivity increase cannot exceed the design lim**it even in the case of **operation outside design limits**.

3a.4.1.1800. Subcriticality shall be **ensured and maintained during any phase** of the storage and transport of fuel elements.

Operating RBMK plants

- In 2006, Rosatom said it was considering lifetime extensions and uprating of its 11 operating RBMK reactors.
  - Following significant design modifications made after the Chernobyl accident, and extensive refurbishment including replacement of fuel channels, a 45-year lifetime is seen as realistic.
  - In 2005, they provided 48% of Russia's nuclear-generated electricity. The R&D Institute of Power Engineering is preparing plans for 5% uprating of them.
- The 'operating until' dates are the scheduled shutdown for these plants, with 15-year lifetime extensions in some cases.
  - Lithuania, on the other hand, closed Ignalina 1 &2 early as a condition for entry into the European Union.
- Russia's long-term plans had earlier included the possibility of replacing the Leningrad units, at the end of their extended service life, by new MKER-1000 units.
  - These are a modification of the RBMK design. The main differences are in the spacing of the graphite lattice in the core and the incorporation of passive safety systems.

Location	Unit	First power	Unit net capacity (MWe)	Status
Lithuania				
Ignalina	1	1983	1185 (originally 1300)	Closed 12/2004
	2	1987	1185 (originally 1300)	Closed 12/2009
Russia				
Kursk	1	1976	925	Operating until 2021
	2	1979	925	Operating until 2024
	3	1984	925	Operating until 2029
	4	1986	925	Operating until 2030
	5	-		Construction suspended
Leningrad	1	1973	925	Operating until 2019
	2	1975	925	Operating until 2021
	3	1979	925	Operating until 2025
	4	1981	925	Operating until 2026
Smolensk	1	1983	925	Operating until 2028
	2	1985	925	Operating until 2030
	3	1990	925	Operating until 2034
Ukraine				
Chernobyl	1	1977	925	Closed 1996
	2	1978	925	Closed 1991
	3	1981	925	Closed 2000
	4	1983	925	Reactor destroyed 1986
	5	-	925	Construction cancelled
	6	-	925	Construction cancelled

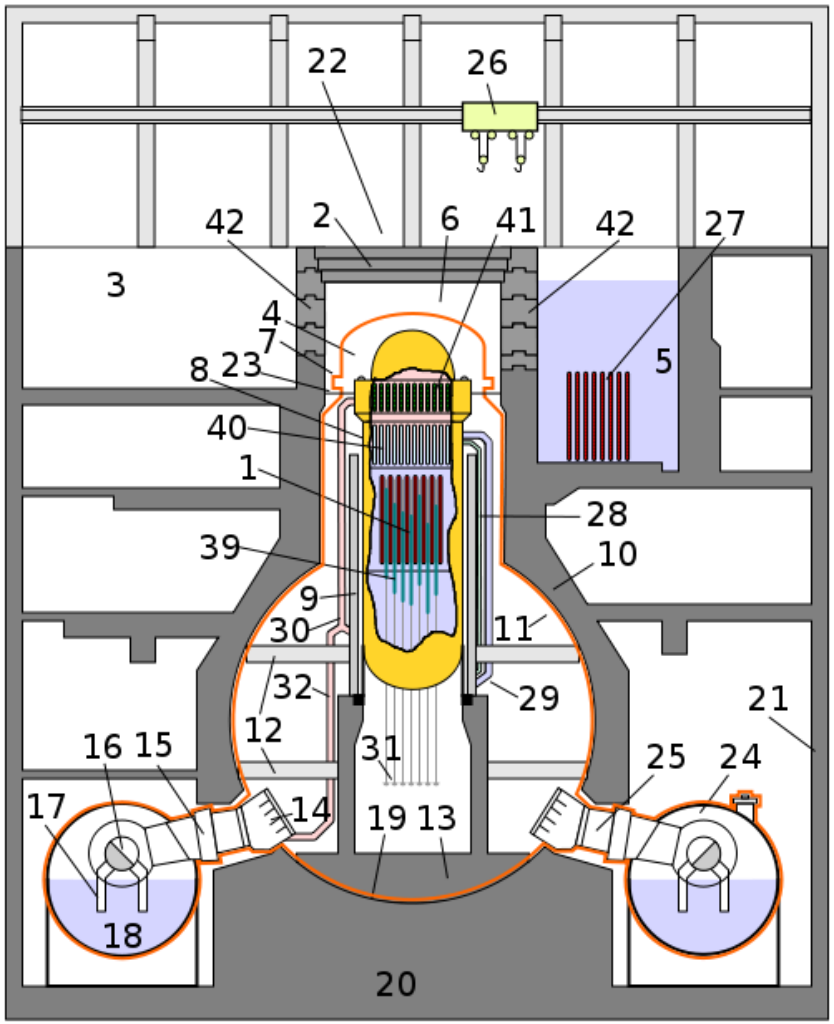
Fukushima Accident

- 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. All three cores largely melted in the first three days.
- The accident was rated 7 on the INES scale, due to high radioactive releases over days 4 to 6, eventually a total of some 940 PBq (I-131 eq).
- Four reactors were written off due to damage in the accident – 2719 MWe net.

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

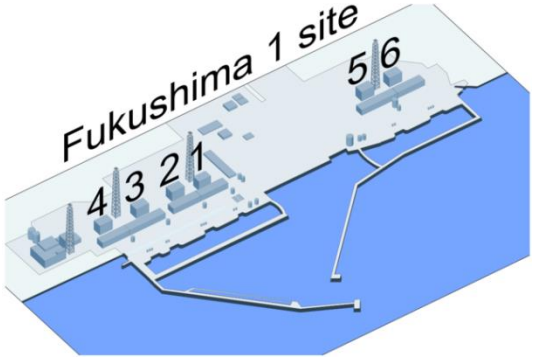
General Electric BWR Mark I containment



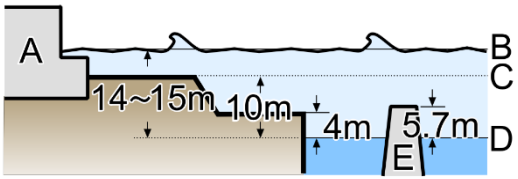
Cross-section sketch of a typical BWR Mark I containment, as used in Units 1 to 5.

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.

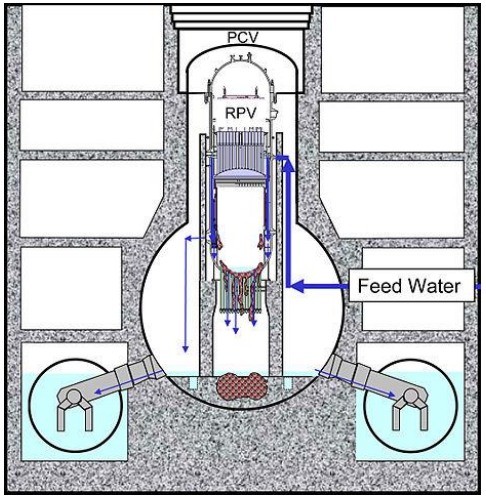
Fukushima Daiichi nuclear disaster



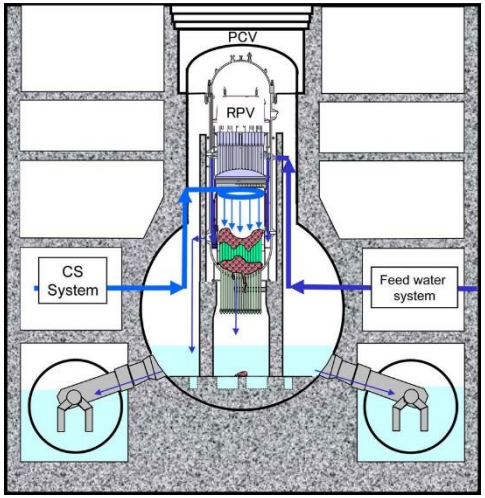
Fukushima Daiichi I nuclear power plant site close-up.



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

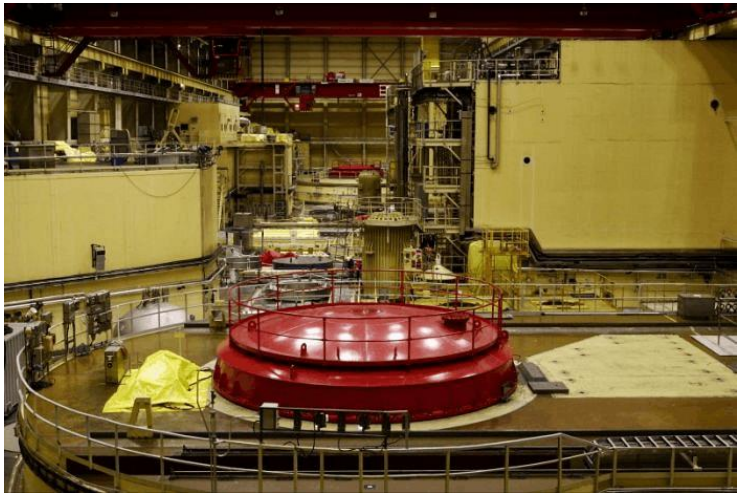
Lessons learned: example requirements

3a.4.3.0800. It shall be demonstrated that **if the cooling capability** of the fuel elements designed for TA1-4 and TAK1 operating conditions **is lost, sufficient time is available to start the alternative cooling** of the fuel elements.

3a.4.3.1000. In the case of systems containing irradiated fuel assemblies, such as the shutdown nuclear reactor or spent fuel pool, **capabilities shall be provided** for **passive heat removal**.

3a.4.3.1100. If the capability of transferring the residual heat to the ultimate heat sink **cannot be demonstrated for every operating condition with high reliability, a secondary ultimate heat sink** and systems required for its operation **shall be provided**, which ensure through their location and design solutions that the heat removal safety function is not lost as a result of external hazard factors.

3a.4.3.1400. The emergency core cooling system shall be so designed that it is **capable of removing the residual heat for the necessary time**. To achieve this, among others, the recirculation of the coolant discharged from the primary circuit to the reactor shall be ensured. …



Serious incident in the Paks Nuclear Power Plant (2003)

- In April 10, 2003 a serious incident occurred in Unit 2 of the Paks Nuclear Power Plant, and a small amount of radioactive material was released into the environment as a result.
- The incident arose from that the fuel assemblies overheated in the cleaning tank, and then cold water was poured on them, and due to this they were severely damaged.

Literature

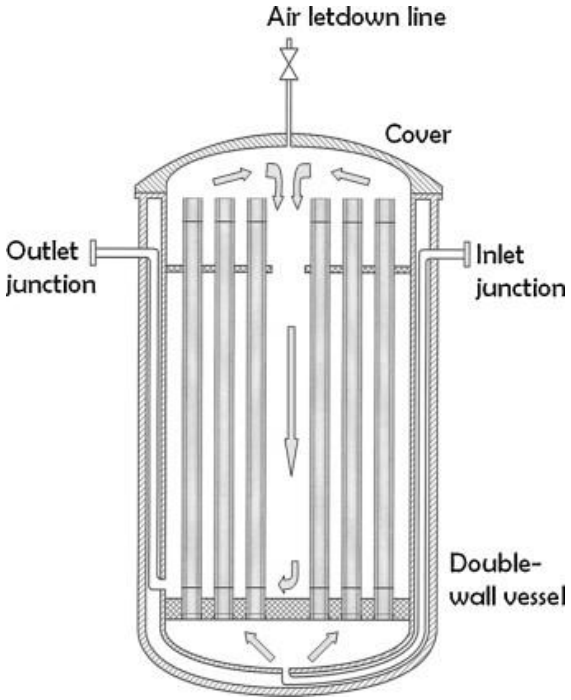
The following slides are based on and some images are taken from the following publications:

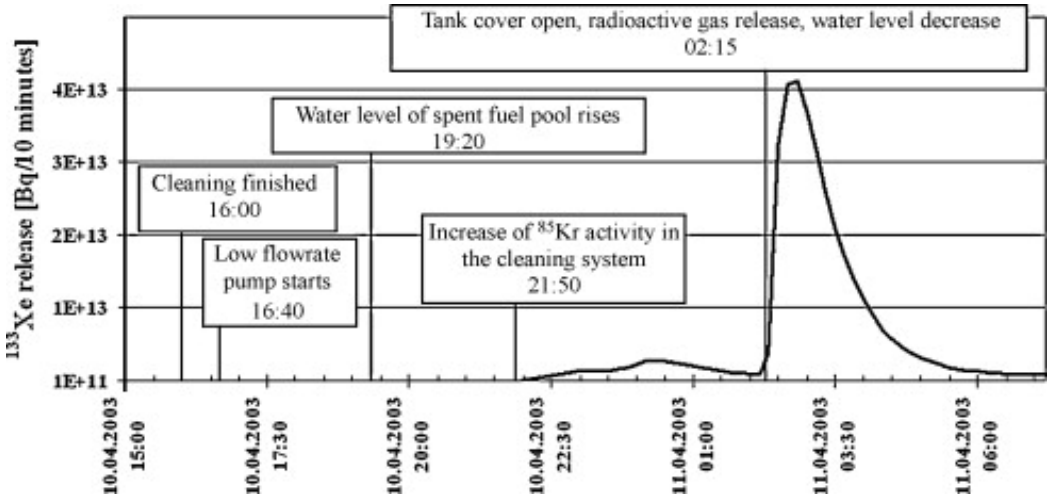
- Szatmáry Zoltán: Súlyos üzemzavar a paksi atomerőműben, Fizikai Szemle 2003/8. 266.o.
- Jelentés az Országos Atomenergia Bizottság Elnöke számára a Paksi Atomerőműben 2003. április 10-én bekövetkezett esemény hatósági kivizsgálásáról (Esemény azonosító: 1120), Országos Atomenergia Hivatal, 2003. május 23.
- L. Vöröss (HAEA, Hungary): Lessons learned from the INES-3 event at PAKS NPP on April 10, 2003, EUROSAFE 2003 Forum, Nuclear Expertise and the Challenge of EU Enlargement, Paris, 25 & 26 November 2003.
- Attila Aszódi, Gábor Légrádi, Ildikó Boros: Causes, course and consequences of fuel damage incident in the Paks NPP, 2003 and connecting thermal-hydraulic analyses, Nuclear Engineering and Design, Volume 240, Issue 3, March 2010, Pages 550-567, ISSN 0029-5493, http://dx.doi.org/10.1016/j.nucengdes.2009.10.008.
- Z. Hózer, et al.: Numerical analyses of an ex-core fuel incident: Results of the OECD-IAEA Paks Fuel Project, Nuclear Engineering and Design, Volume 240, Issue 3, March 2010, Pages 538-549, ISSN 0029-5493, http://dx.doi.org/10.1016/j.nucengdes.2009.09.031.

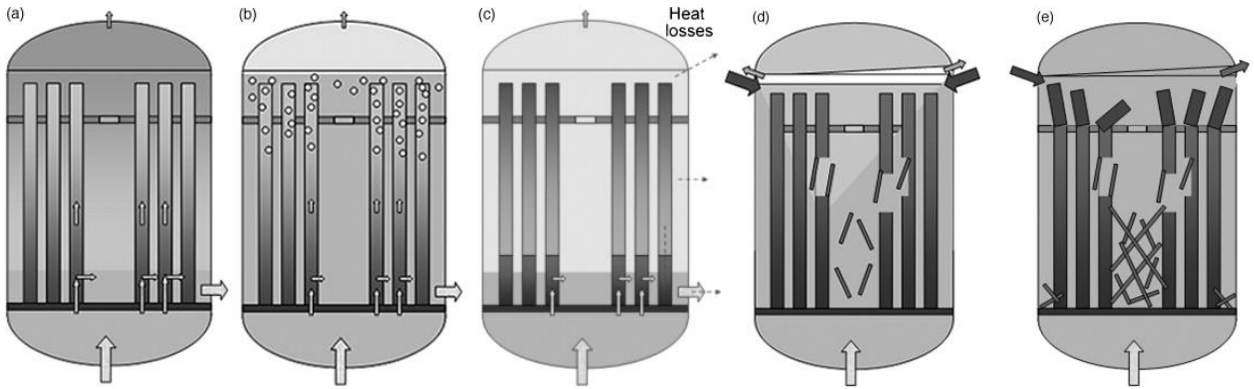
Chronology of the main events

Time	Occurrence
April 10, 2003	
16:00	The cleaning of the 6th batch (30 assemblies, just taken out of the reactor) was finished. However, the assemblies were not removed from the cleaning tank, because the crane required for the lifting of the lid of the tank was still busy with other tasks.
16:40	The AMDA was switched to «B» operating mode. Cooling of the fuel assemblies was ensured with the submersible pump circulating the water inside the service shaft.
21:50	The counts on the Kr-85 measuring device of the AMDA system suddenly increased.
21:53	The warning limit was reached on the noble gas detector placed on the reactor platform of Unit 2, the measured value was 1700 kBq/m^3.
22:50	The head of the Dosimetry Service evacuated the reactor hall.
23:45	The measured value on the noble gas detector placed on the reactor platform was 26100 kBq/m^3. Following the instructions of the Shift Supervisor the maintenance ventilation systems of the reactor hall were started, the ventilation of the reactor hall operated with full capacity.
April 11, 2003	
2:15	The hydraulic locks, which ensure the leak tight closing the lid of the cleaning tank were loosened by the technician of the FANP. Simultaneously with the loosing of the lid of the cleaning tank the gamma dose rate significantly increased in the vicinity of the spent fuel pool and the service shaft (6-12 mSv/h).
12:40	The Safety Director ordered partial alerting of the Emergency Preparedness Organisation (telecommunication, radiation assessment groups).
13:15	The Shift Supervisor initiated measures in order to decrease the release to the environment.
April 16, 2003	
16:23	The lid of the cleaning tank was lifted. No increase was observed on the radiation measuring (SEJVAL) system.
20:00	It was found during the visual observation, (using remote control camera), that the fuel elements inside the tank were significantly damaged.
22:30	The Paks NPP declared stage “ALERT” and alerted its Emergency Preparedness Organisation.
April 19, 2003	
10:00	The boric acid concentration in the spent fuel pool was increased to the value of 16 g/kg in order to ensure the appropriate sub-criticality. The reliability of the cooling system of the cleaning tank was ensured by the newly installed pump provided so higher redundancy. One of the pumps was sufficient for cooling while the other one served as reserve.
April 20, 2003	
9:00	The Safety Director terminated the operation of the Emergency Preparedness Organisation.

What happened in the cleaning tank?

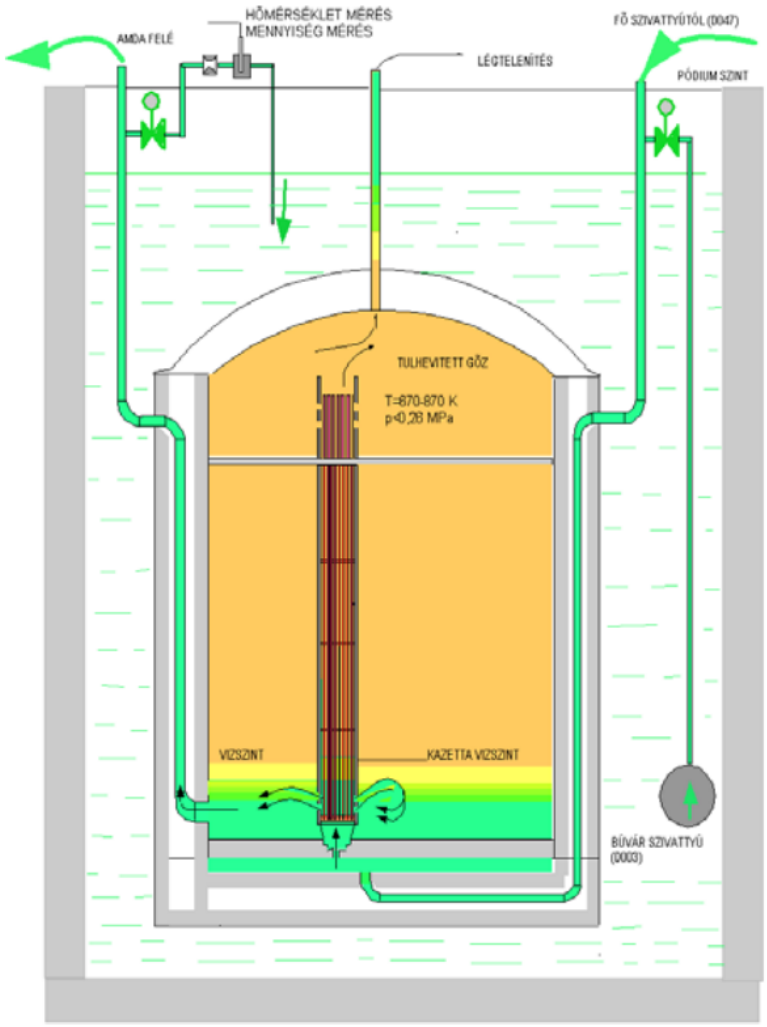






The reasons behind the incident

- the outlet of the inner tank was at the bottom
- the holes in the walls of the fuel assembles were disregarded in the thermo-hydraulic design and analyzes
- the cross-section of the air vent was too small
- the sustained operation in operating status B
- the failure to open the lid early
- the imprecise fitting of the lower end of the fuel assemblies (potential)
- the complete lack of instrumentation in the tank, in particular the missing measurement of the temperature under the lid
- the lack of continuous collection of measurement data (this would have allowed earlier detection of the problems)
- the lack of evaluation of the difference in the outlet water temperature of the tank and the near-surface water temperature of the shaft
- only an imprecise measurement tool was available to notice changes in the level of the pool, and no one was monitoring it



Lessons learned: example requirements

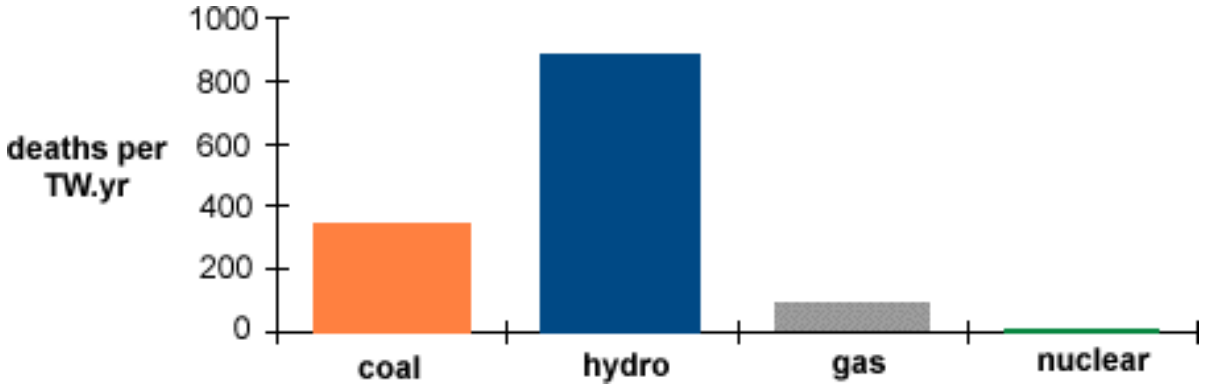
3a.4.5.1400. Instrumentation suitable for the measurement of parameters **necessary for monitoring fundamental safety functions** shall be provided, thus ensuring the availability of information necessary for the reliable and safe operation of the nuclear power plant unit and the management of events resulting in TA2-4 and TAK1 and TAK2 operating conditions.

3a.4.5.1700. Monitoring and measurement instrumentation **shall be provided for the observation of the locations where radioactive materials are present** and for the measurement of their quantities in all locations where they may be released into the environment.

3a.4.5.2300. **Appropriate hazard signals** that allow intervention by the operating personnel **before the given parameters would reach the set values triggering** the operation of the safety protection systems shall be applied. The signals associated with protection operations or important parameter deviations **shall be supplied with sound alarms** both in the unit main and backup control rooms. The signals associated with protective operation shall be acknowledgeable only by the intervention of the operating personnel even after the limit is no longer exceeded.

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