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

Nuclear Power Plant Safety Basics

Construction Principles and Safety Features on the Nuclear Power Plant Level

Safety of Nuclear Power Plants

Overview of the Nuclear Safety Features on the Power Plant Level

Characteristics of Nuclear Power Plants

- They contain a large amount of radioactive material
- Employees need to be protected from radiation even in normal operation
- The release of radioactive contaminants must be prevented even in accident conditions!
- Plans must exist to handle the problems if radioactive contaminants are still released
- Residual (decay) heat removal (heat from the decay of fission products) is of high importance

Safety Goals of Nuclear Power Plants

- Normal operational state: intrinsically safe
  - environmentally safe: no release of contaminants
  - intrinsic safety: negative void coefficient

But

- Potentially hazardous
  - possibility of severe consequences due to an incident
  - design flaws and incompetence can lead to accidents
- Aim: avoidance of accidents
  - design and build a safe nuclear power plant
  - safe operation and maintenance of the NPP

Safety of Nuclear Power Plants

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

- Nuclear safety has three objectives:
    1. to ensure that nuclear facilities operate normally and without an excessive risk of operating staff and the environment being exposed to radiation from the radioactive materials contained in the facility
    2. to prevent incidents, and
    3. to limit the consequences of any incidents that might occur
- Aim: to guarantee in every possible operational and accident conditions (above a certain occurrence frequency and consequence, i.e. risk) that the radioactive material from the active zone be contained in the reactor building

Safety of Nuclear Power Plants

- Nuclear power plants and its safety systems and technical equipment must be designed so that the safety of the environment is guaranteed even if an accident occurs
- Modern nuclear power plants satisfy these criteria
- Periodic safety audits are required to
  - assess the effectiveness of the safety management system
  - and identify opportunities for improvements
- The licensing authority permits the startup, operation or maintenance of a nuclear power plants only if the guaranteed safety of the reactor is proven

The Basic Principles of Nuclear Safety

- Nuclear safety uses two basic strategies to prevent releases of radioactive materials:
  1. the provision of leak tight safety „barriers"
  2. the concept of defense-in-depth
     - applies to both the design and the operation of the facility
  - despite the fact that measures are taken to avoid accidents, it is assumed that accidents may still occur
  - systems are therefore designed and installed
    - to combat them, and
    - to ensure that their consequences are limited to a level that is acceptable for both the public and the environment

Five Layers of Safety Barriers in NPPs

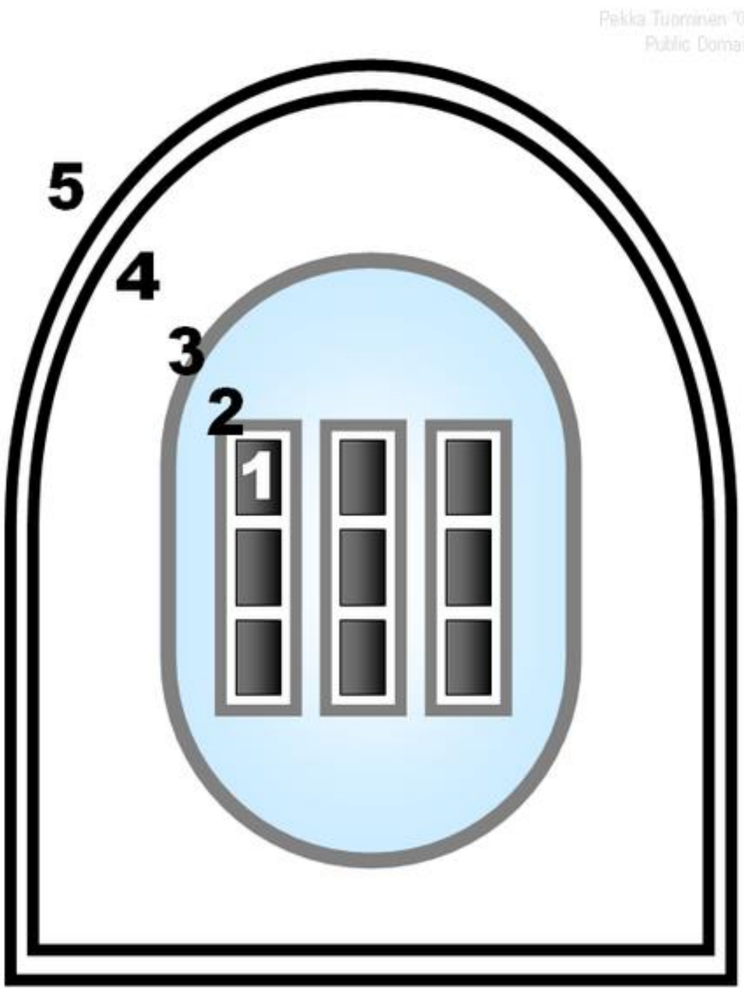
1st layer is the inert, ceramic quality of the uranium oxide

2nd layer is the air tight zirconium alloy of the fuel rod

3rd layer is the reactor pressure vessel made of steel

4th layer is the pressure resistant, air tight containment building

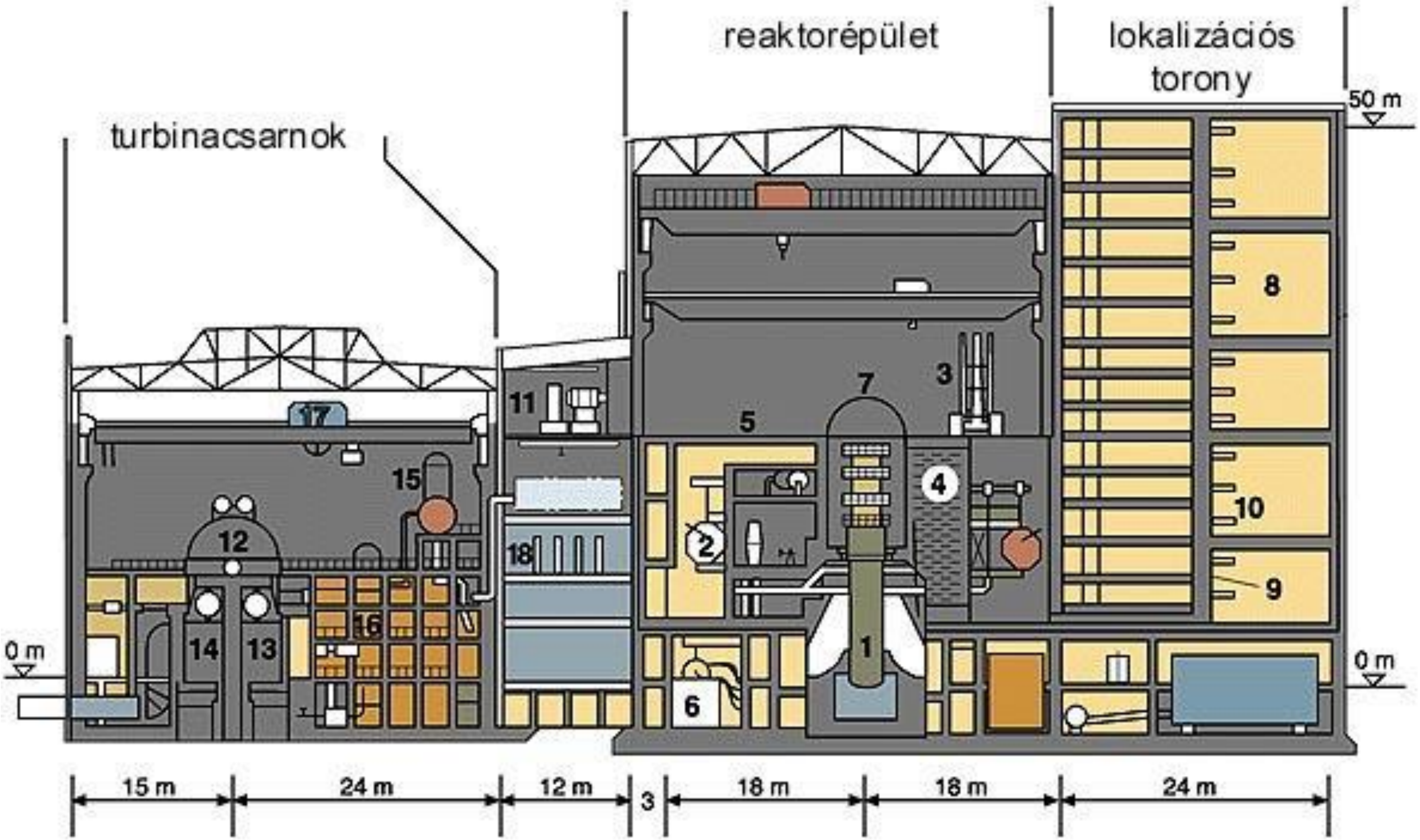
5th layer is the reactor building or a second outer containment building



Pressure Resistant, Air Tight Containment

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

Structure of the Paks NPP and Safety Barriers



Main Systems Shown in the Previous Figure

1. Reactor vessel
2. Steam generator
3. Refuelling machine
4. Cooling pond
5. Radiation shield
6. Supplementary feedwater system
7. Reactor
8. Localization tower
9. Bubbler trays
10. Deaerator
11. Aerator
12. Turbine
13. Condenser
14. Turbine hall
15. Degasser feedwater tank
16. Feedwater pre-heater
17. Turbine hall overhead
18. Control and instrument room

Levels of Defence in Depth

Level 5: Mitigation of radiological consequences of significant releases of radioactive materials

Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents

Level 3: Control of accidents within the design basis

Level 2: Control of abnormal operation and detection of failures

Level 1: Prevention of abnormal operation and failures

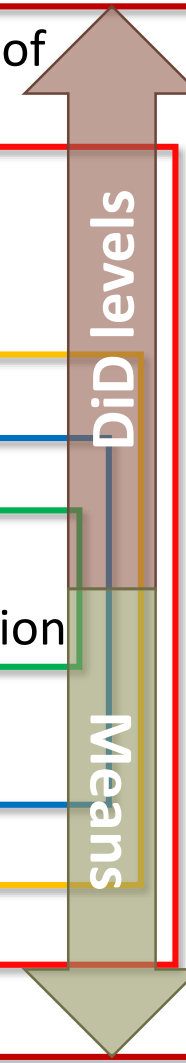
Conservative design and high quality in construction and operation

Control, limiting and protection systems and other surveillance features

Engineered safety features and accident procedures

Complementary measures and accident management

Off-site emergency response



Correlation between DiD levels and the allocation of events/PIEs

		Operational States (OS)		*Accident Conditions (AC)*			
IAEA SSR 2/1		**Normal Operation**	**Anticipated operational occurrences**	**Design basis accidents (DBA)**		**Design Extension Conditions** *(without significant fuel degradation*	**Severe accidents** *(with core melting)*
WENRA	DiD Level 1	Prevention of Abnormal operation and failure					
	DiD Level 2		Control of Abnormal operation and failure				
	DiD Level 3.a			Control of accident to limit radiological releases and prevent escalation to core...			
	DiD Level 3.b					...damage conditions	
	DiD Level 4						Control of accidents with core melt to limit offsite releases
	DiD Level 5						Mitigation of radi.
Design Base Conditions / Design Extension Conditions		DBC-1	DBC-2	DBC-3	DBC-4	DEC-A	DEC-B
		Transients related to normal operation	Anticipated operational occurrences	Infrequent accidents	Limiting accidents (higher frequency) (lower frequency)	Reduction of risk and prevention of core meltdown	Reduction of risk and control of core meltdown
Frequency		Each event in this category is expected to occur frequently or regularly during operation	Each PIE in this category should be expected to occur one or a few times during plant lifetime	No individual PIE in this category is expected to occur during the plant lifetime, but one or a few PIE within this category should be expected during plant lifetime	PIEs in this category are considered to be possible but are believed to be excluded by the design. Nevertheless, they are considered on order to understand the radiological consequences of limiting accidents	PIEs in this category are not considered to be sufficiently credible to include as design basis events but are nevertheless considered in the design process inorder to ensure radioactive releases are kept within acceptable limits should they occur.	
		f>1/a	f<10-	10^{-2}/a<f10^{-3}/a	f<10^{-3}/a	10^{-4}/a<f<10^{-6}/a	CDF<10^{-5}/a;LRF< 5*10^{-7}/a

Source: Safety Classification for I&C Systems in Nuclear Power Plants – Current Status & Difficulties — CORDEL Digital Instrumentation & Control Task Force

Design Limits – Design Basis Accidents

- The design limits prescribe that for any DBA:
  - the fuel cladding temperature must not exceed 1200°C
  - the local fuel cladding oxidation must not exceed 18% of the initial wall thickness
  - the mass of Zr converted into ZrO_2 must not exceed 1% of the total mass of cladding
  - the whole body dose to a member of the staff must not exceed 50 mSv
  - critical organ (i.e., thyroid) dose to a member of the staff must not exceed 300 mSv

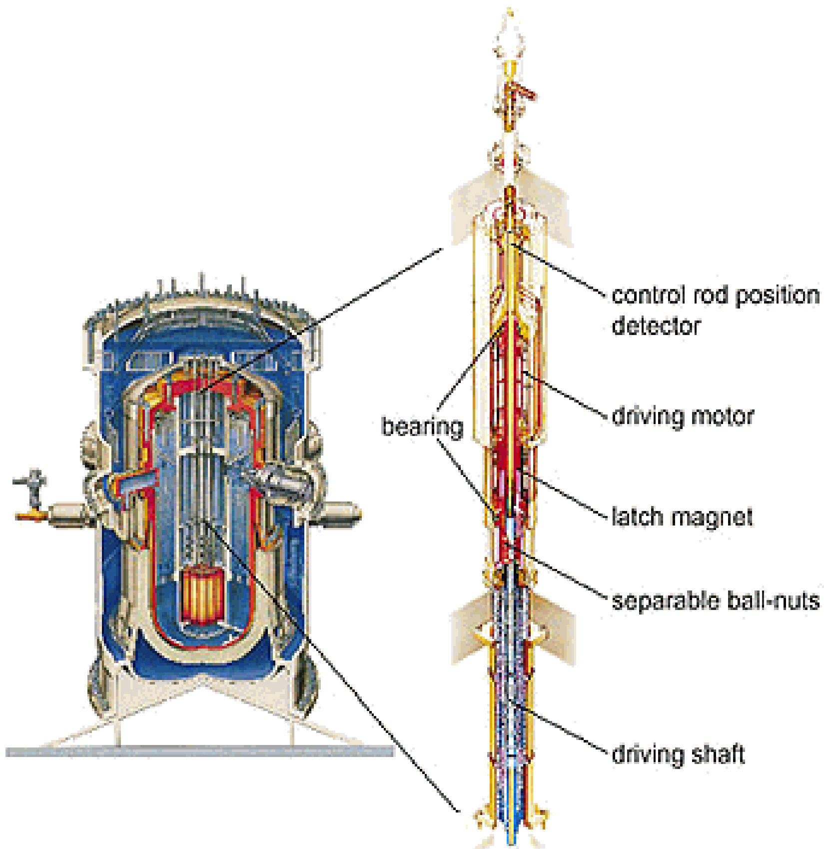
Safety Functions

- Their purpose is to ensure safety
  - in operational states
  - in and following a design basis accident, and
  - (to the extent practicable) on the occurrence of selected BDBAs (beyond design basis accidents)
- The following fundamental safety functions shall be performed:
  1. control of the reactivity
  2. removal of heat from the core
  3. confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases

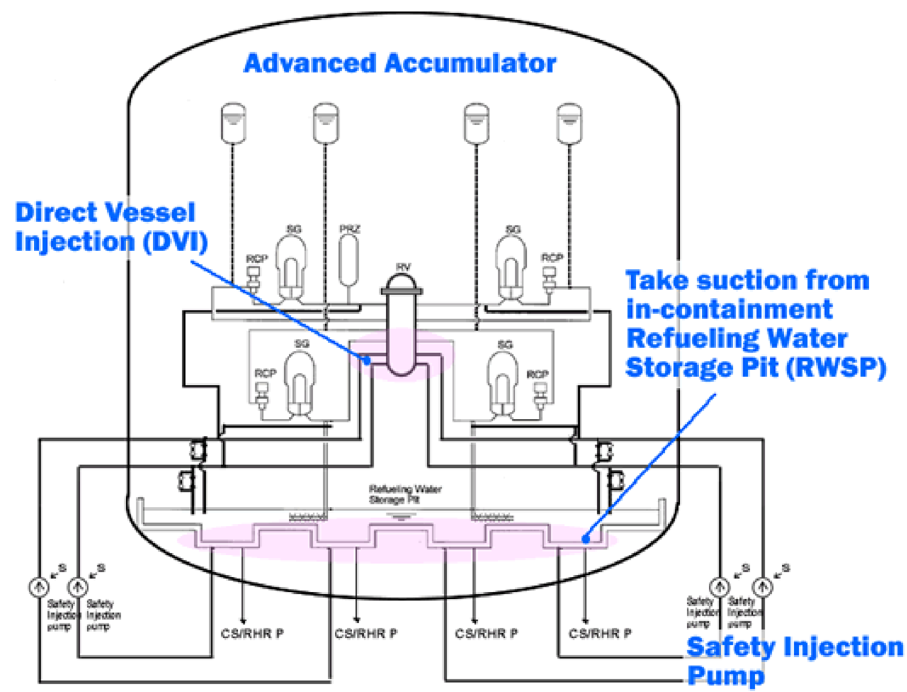
Main Safety Systems in Nuclear Power Plants

- Reactor Protection System (RPS)
  - Control Rods
  - Safety Injection / Standby Liquid Control
- Emergency Core Cooling System
  - High Pressure Coolant Injection System (HPCI)
  - Depressurization System (ADS)
  - Low Pressure Coolant Injection System (LPCI)
  - Core spray and Containment Spray System
  - Isolation Cooling System
- Emergency Electrical Systems
  - Diesel Generators
  - Motor Generator Flywheels
  - Batteries
- Containment Systems
  - Fuel Cladding
  - Reactor Vessel
  - Primary and Secondary Containment
- Ventilation and Radiation Protection

Main Safety Systems in Nuclear Power Plants

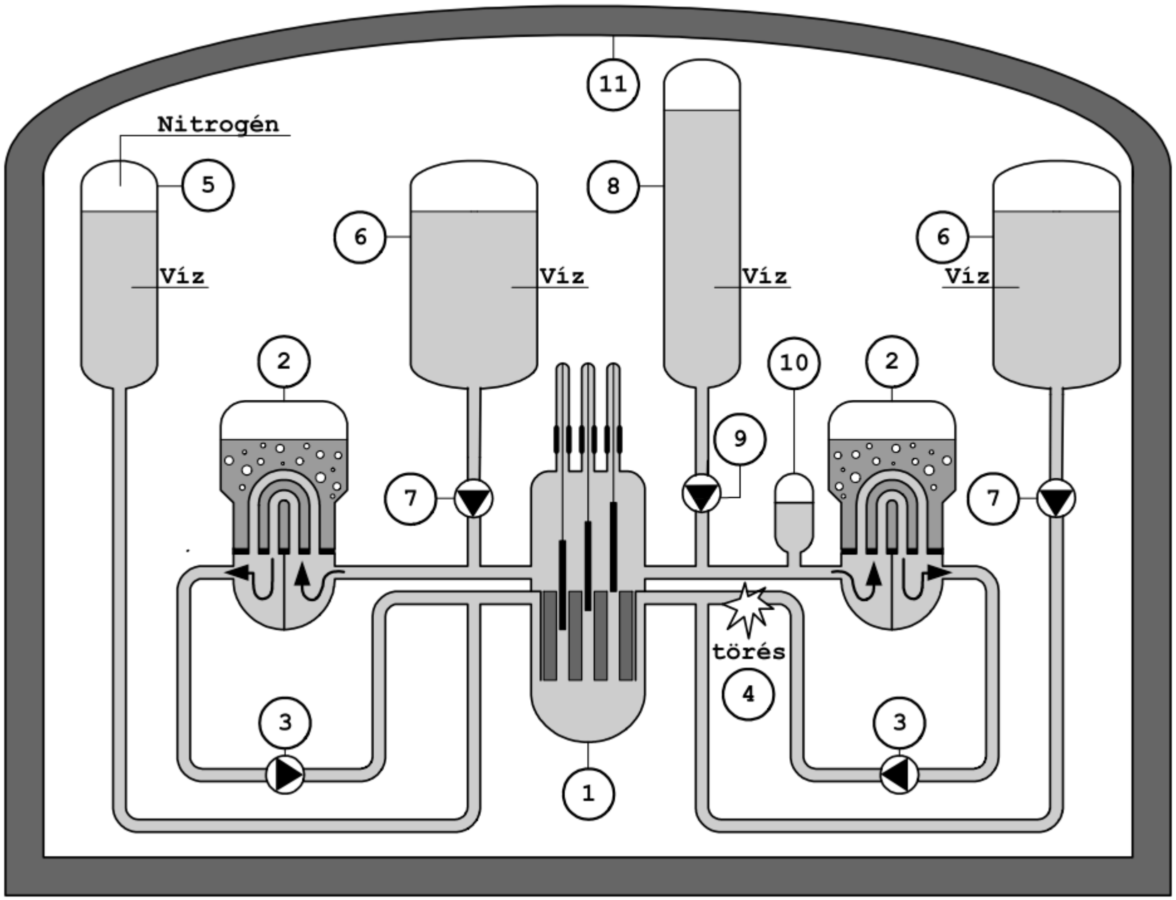


Control Rods



Emergency Core Cooling System

Emergency Core Cooling System



1. Reactor
2. Steam Generator
3. Main Cooling Pump
4. Primary Pipe Rupture
5. Hidroaccumulator
6. Low Pressure Coolant Injection System Vessel
7. Low Pressure Coolant Injection System Pump
8. High Pressure Coolant Injection System Vessel
9. High Pressure Coolant Injection System Pump
10. Pressurizer

Safety Features of Modern NPPs

Requirements for a New Reactor Build

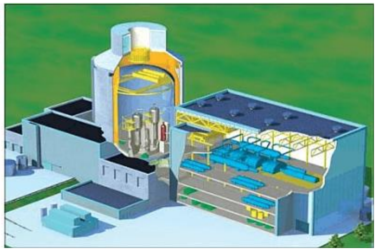
Possible Reactor Unit Types and their Safety Features

Requirements for a New Reactor Build

- Main aspects:
  - Safety aspects
    - CDF < 10^{-5}/year
    - technical solutions for severe accidents
  - Technical aspects
    - Generation III+
    - no prototype reactor
    - at least 60 years lifetime with >90% availability
  - Economical aspects
    - Competitive generating cost (short construction period!)
    - Financing of the construction

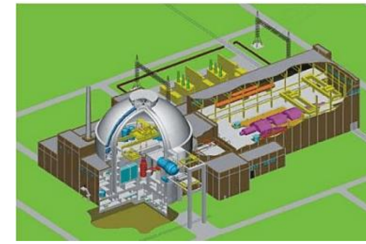
- Possible reactor types and vendors:
  - AP1000 (Westinghouse)
  - AES-2006 (Atomstroyexport)
  - EPR (Areva)
  - ATMEA (Areva-Mitsubishi)
  - APR1400? (KHNP)

Possible Reactor Types and Vendors



Toshiba-Westinghouse AP1000

- Modular construction
  - 1100MWe PWR
  - Passive safety systems
- At least four units under construction in China
- Currently being evaluated in UK Generic Design Assessment
- One novel aspect is the use of explosive 'squib' valves

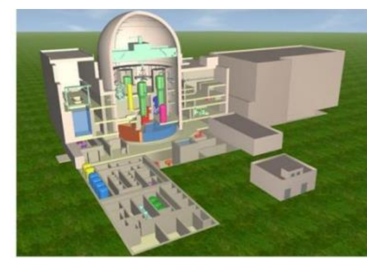


Atomstroyexport AES-2006

- Developed from earlier VVER-1000 designs
  - 1150 MWe
  - Includes some passive safety features
- 4-loop design, horizontal steam generators
- Advanced safety features including 72 hour site blackout capability

Areva European Pressurised Water Reactor (EPR)

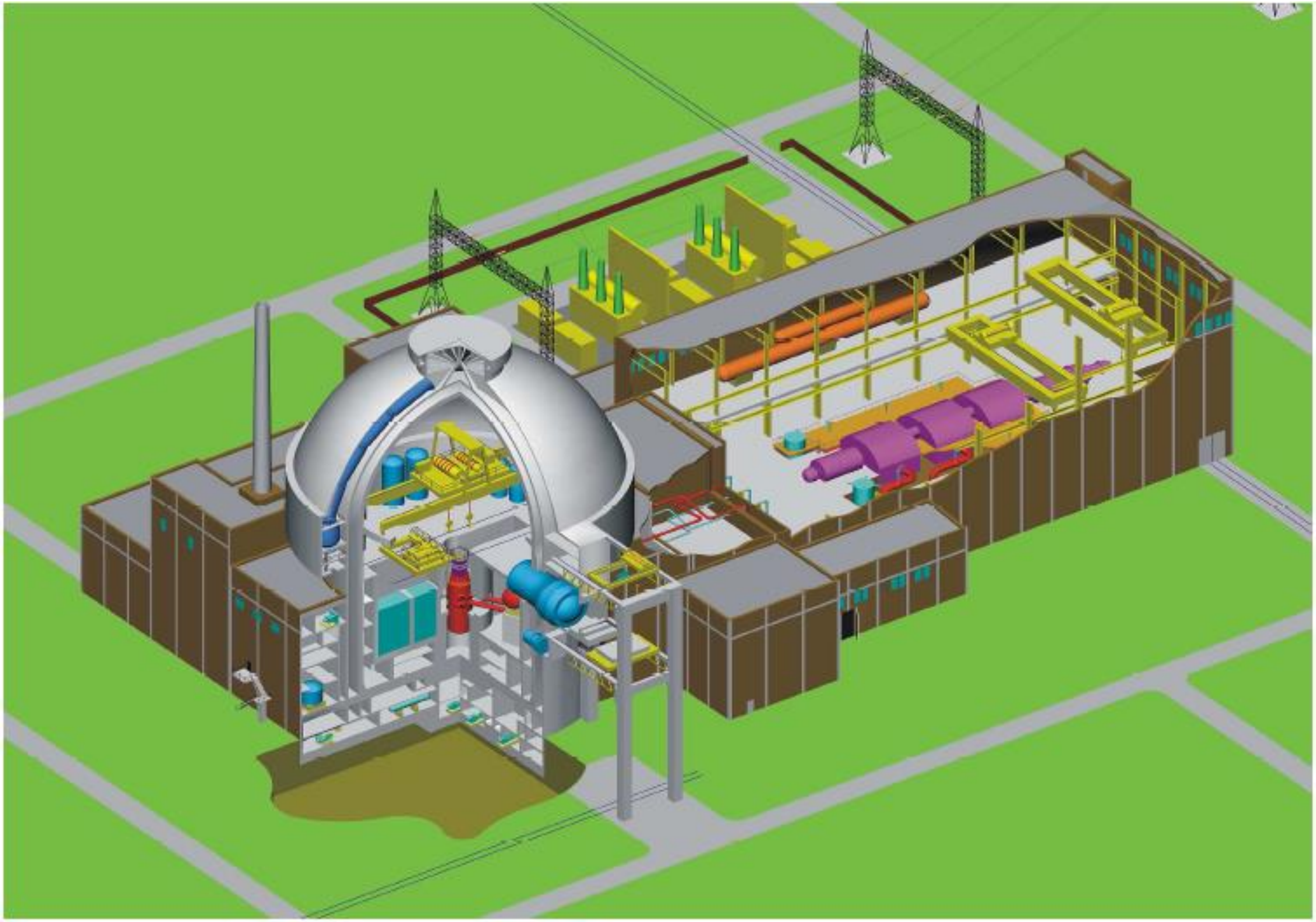
- Based on French N-4 and German Konvoi
  - 1600 MWe
  - Advanced safety systems
- First EPR is close to completion in Finland
- Construction in progress in France and China
- More are planned in France and the UK



Areva-Mitsubishi designed ATMEA

- Based on 900MWe Framatome-EdF unit design
  - 1100MWe plant, 3-loop
  - Claimed Generation III+ safety features
- Load-following design
- Smaller size (than EPR) for countries with smaller grids
- No orders yet (Jan 2012)

Arrangement of the AES-2006 Unit



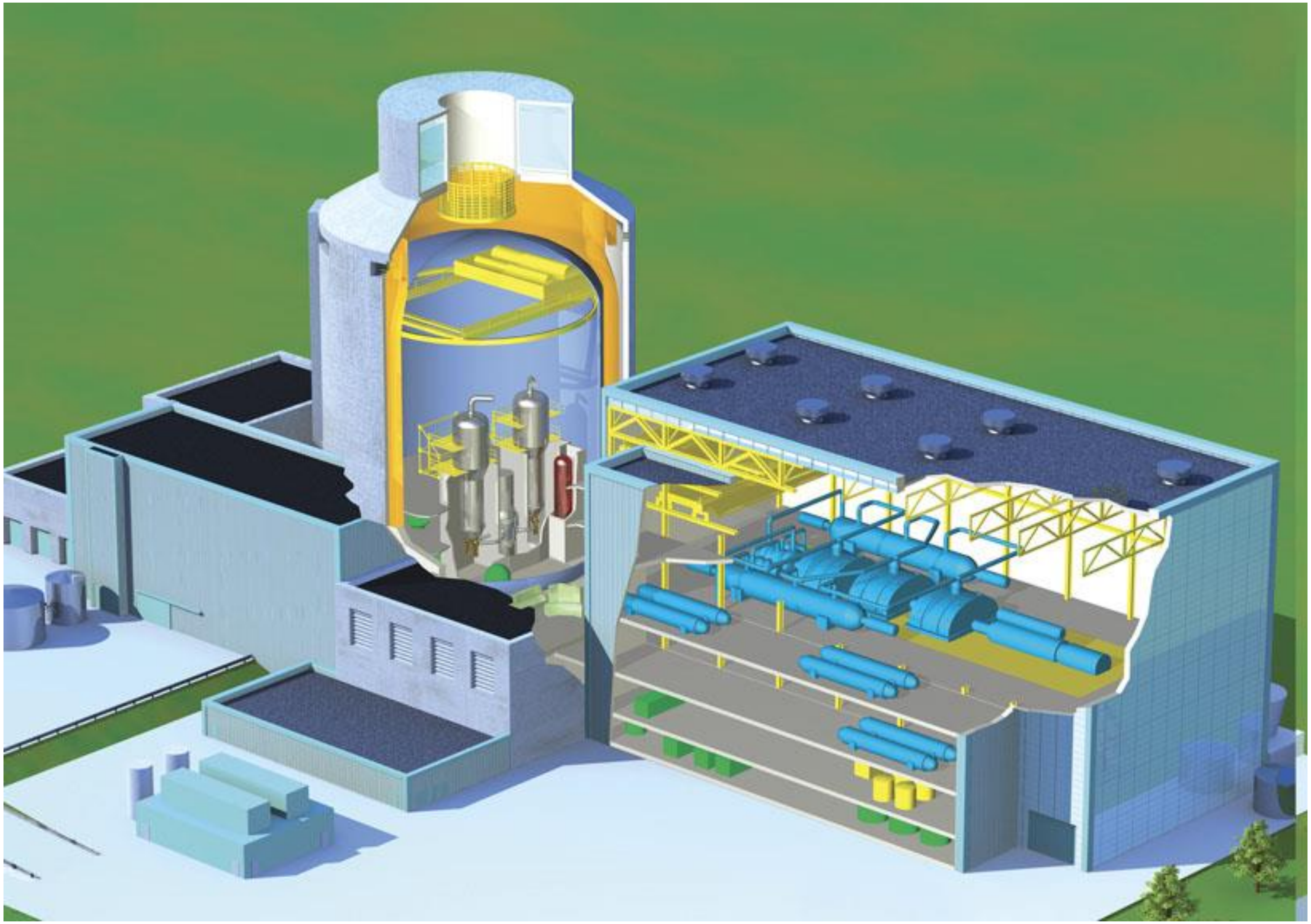
Containment of the AES-2006 Unit

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

Safety features:

- 4×100% ECCS redundancy
- Active and passive protection systems
- Core catcher
- Digital I&C
- Advanced protection against external initiating events

Arrangement of the Westinghouse AP1000 Unit

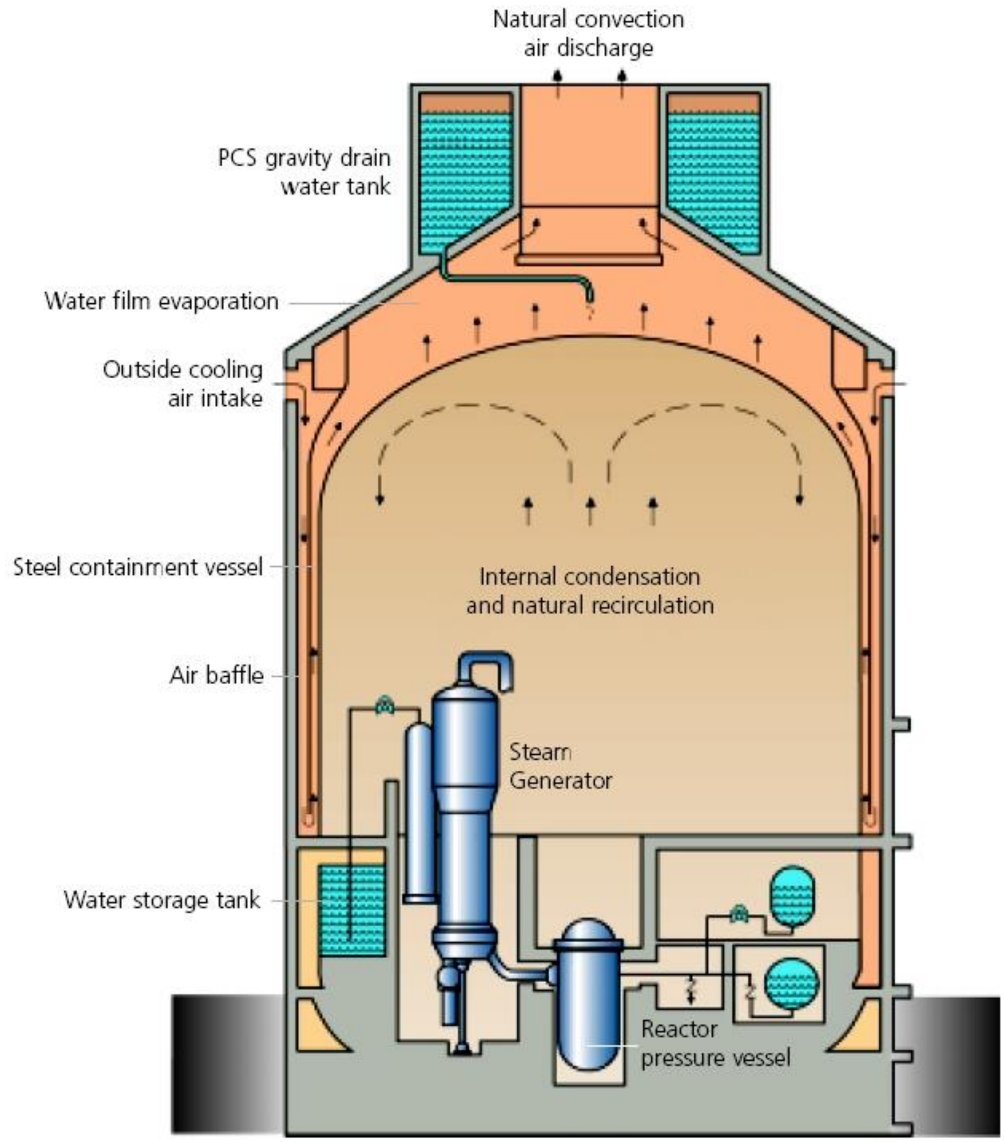


Containment of the AP1000 Unit

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

Safety features:

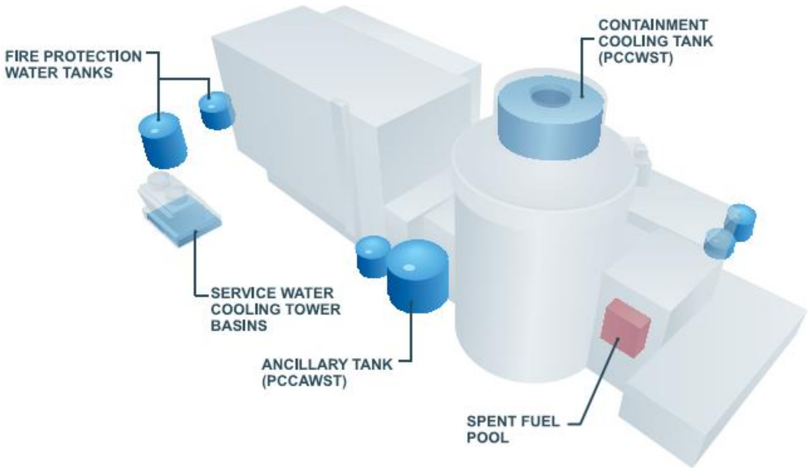
- 2×100% ECCS redundancy
- Passive protection systems
    - Passive ECCS
    - Emergency spray
    - Natural circulation and decay heat transfer
    - Containment cooling
- External cooling of the reactor vessel
- Digital I&C

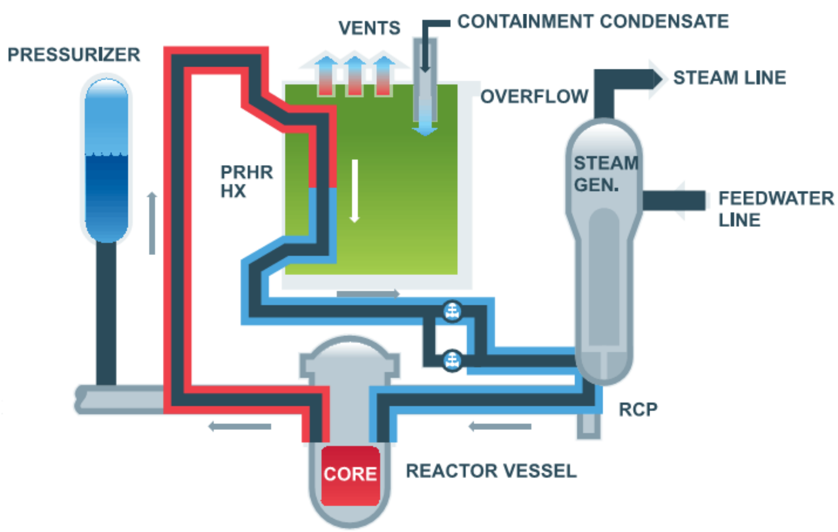


The Passive Containment of the AP1000 Reactor Unit

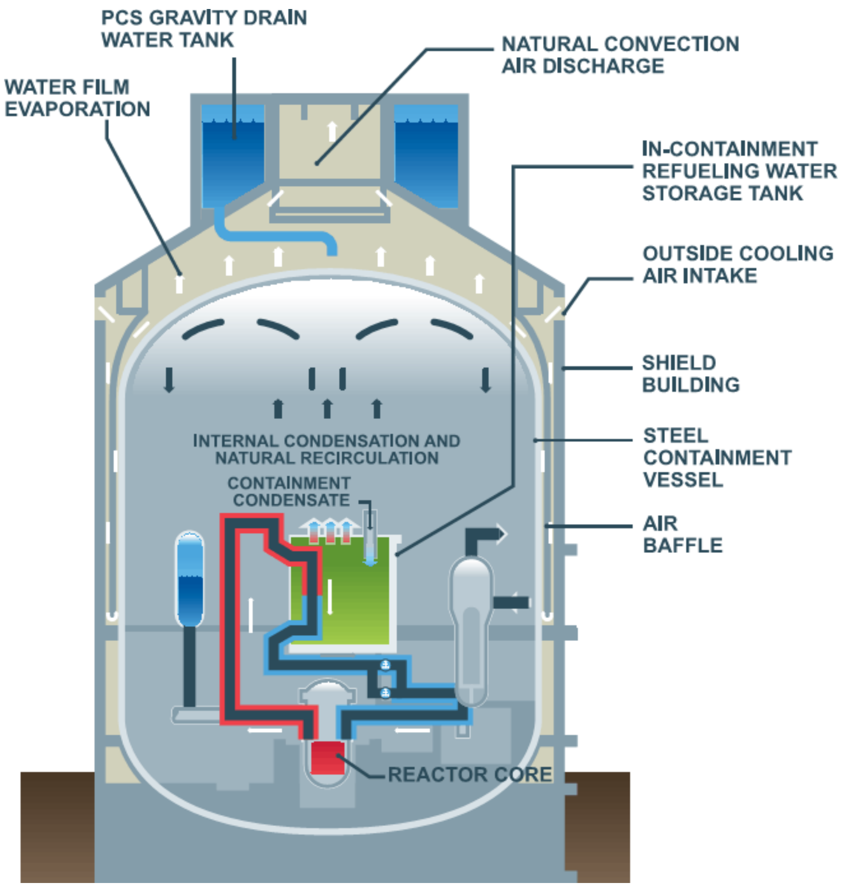
AP1000 Unit Passive Safety Features

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





Natural circulation and decay heat transfer



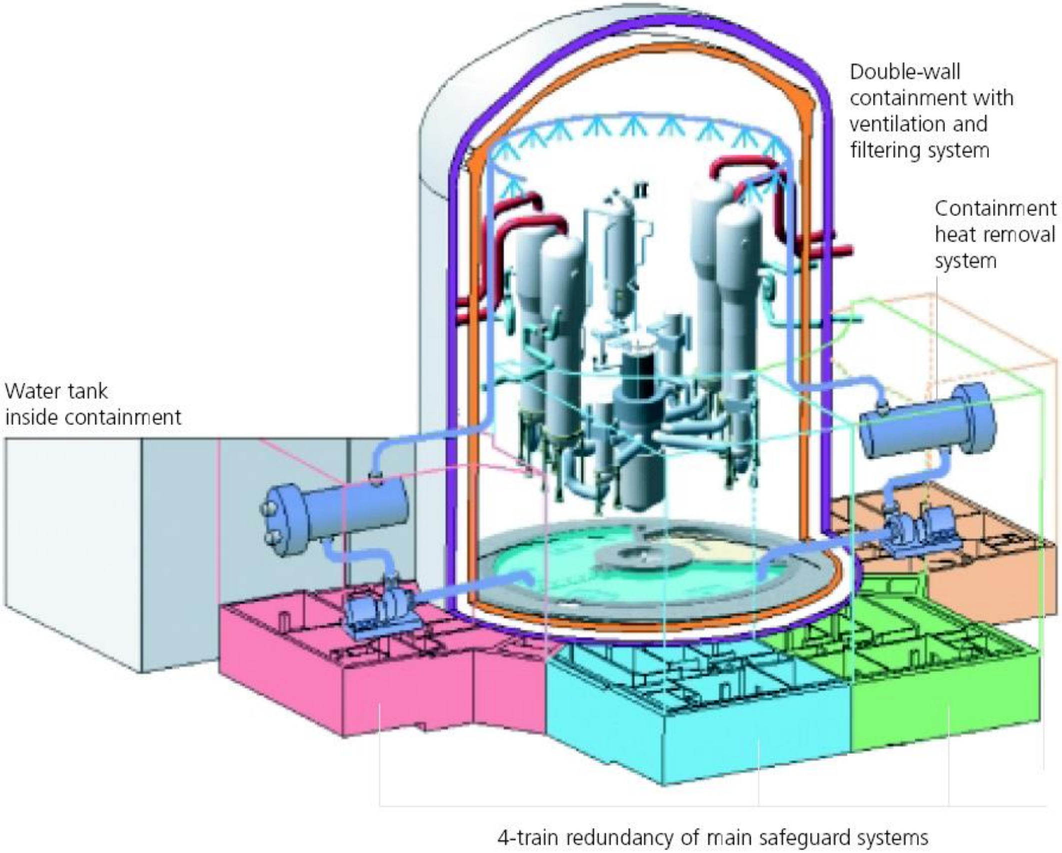
Transfer of reactor decay heat to outside air

Arrangement of the Areva EPR near Olkiluoto

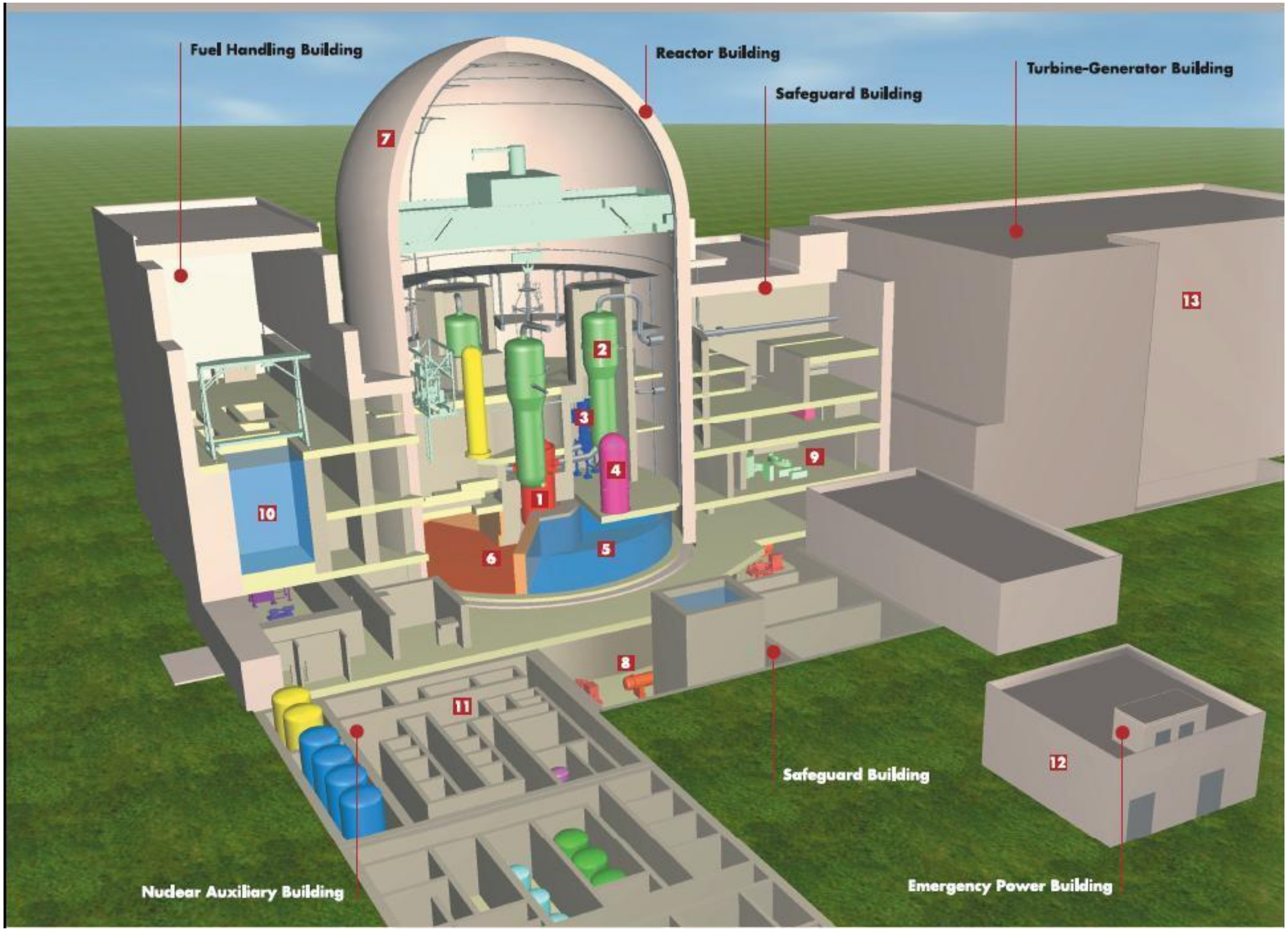
Containment of the EPR Unit

Safety features:

- 4×100% ECCS redundancy
- Active and passive protection systems
- Large water storage tank (in containment) for passive flooding of the core
- Core catcher
- Digital I&C
- Protected from the crash of a large airliner



Arrangement of the Areva-Mitsubishi ATMEA



Containment of the ATMEA Unit

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

Safety features:

- 3×100% ECCS redundancy
- Active and passive protection systems
  - E.g. “advanced” hidroaccumulators
- Core catcher
- Digital I&C
- Advanced protection against external events
  - E.g. airliner crash, earthquake