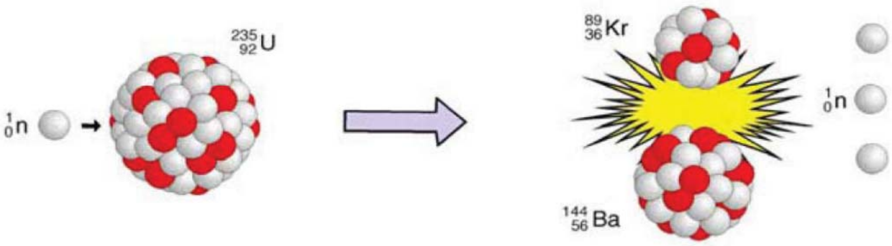
Safety of Nuclear Power Plants

Basic Safety Problem and Safety Philisophy («Defense-in-Depth"), Design Principles, Accident Management, Trends

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
Laboratory for Safety Analysis
INSTITUTE FOR ENERGY TECHNOLOGY
DMAVT
Departement Maschinenbau & Verfahrenstechnik;
Department of Mechanical & Process Engineering

Exemplary nuclear fission equation



$$^{235}_{92}U + ^{1}_{0}n \longrightarrow ^{89}_{36}Kr + ^{144}_{56}Ba + 3\,^{1}_{0}n + 210\ \text{MeV}$$

(80% kinetic energy)

- **3,1 · 10^{10} fissions per sec for 1 W**

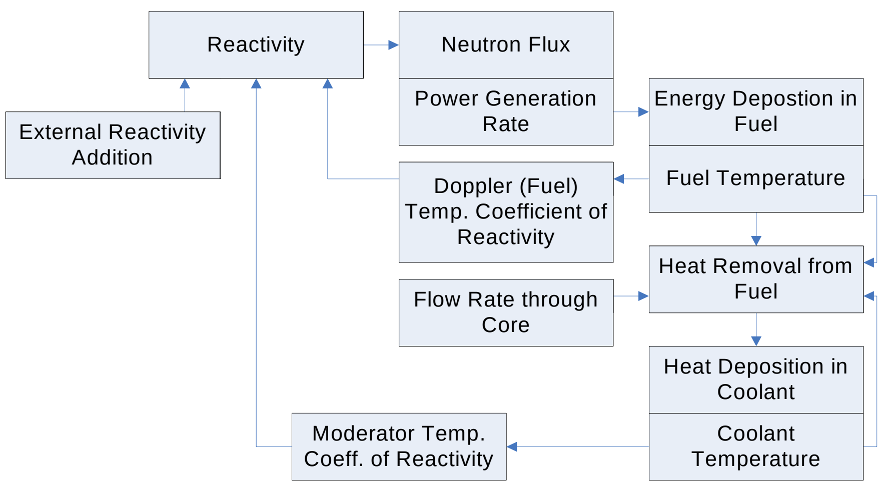
Source: Forschungszentrum Karlsruhe

Safety Problem

The primary danger lies within the high core inventory of radioactive substances. Those substances released to the environment, even in fractional amounts, endanger health.

Spaltprodukte	Isotope	Halbwertszeit	Aktivität [kBq/cm³]	Emission	Biologische Effekte und kritische Organe
Metalle – Nicht flüchtig	Sr^{89}	53 d	92.5×10^{-3}	β^-	Ingestion und Fixierung in den Knochen
Metalle – Nicht flüchtig	Sr^{90}	28 a	1.65×10^{-3}	β^-	
Metalle – flüchtig	Cs^{137}	2.1 a	2.59	β^-, γ	Ganzer Körper
	Cs^{134}	30 a	15.9	β^-	
Halogene (flüchtig)	I^{129}	1.7×10^{9} a	-	β^-, γ	Inhalation und Fixierung in der Schilddrüse
	I^{131}	8 d	55.5	β^-, γ	
	I^{133}	21 h	92.5	β^-, γ	
Spaltprodukte ohne Edelgase			473.6		
	Kr^{85}	10.6 a	40.7	β^-, γ	Häuptsächlich externe Bestrahlung, Inhalation
Edelgase	Kr^{88}	2.8 h	96.2	β^-, γ	
	Xe^{133}	5.3 d	6438	β^-, γ	
Total Spaltprodukte			7048.5		

Reactivity Induced Accidents (RIA): Simplified Representation of Feedback Mechanisms in a LWR

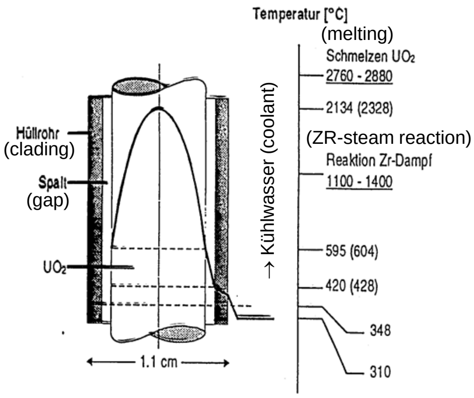


ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Laboratory for Safety Analysis
INSTITUTE FOR ENERGY TECHNOLOGY

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Temperature Distribution in a Fuel Rod of a Pressurised Water Reactor at Nominal Power



In case of criticality accidents, the energy is deposited in the fuel and leads to its fragmentation. Such conditions can occur if the absorber is lost, e.g. in case of dilution of the boron solved in the cooling water or withdraw of the absorber rods.

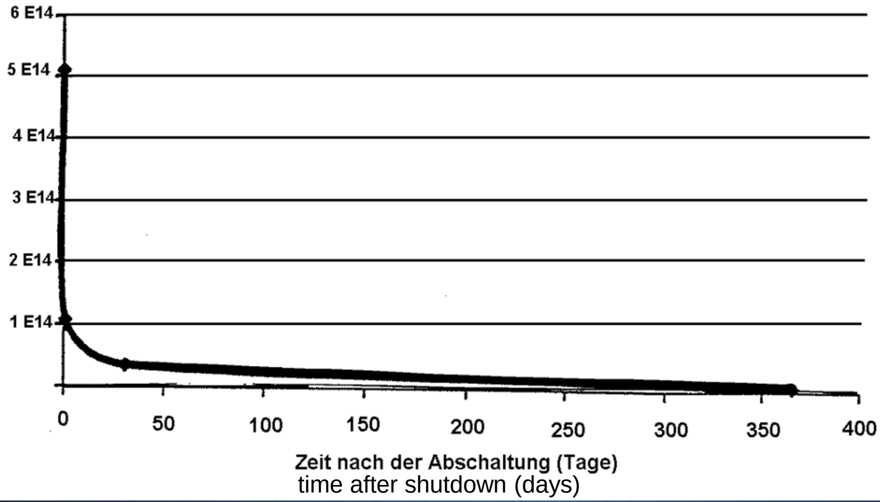
In case of insufficient cooling of the core, fuel / fuel elements can be overheated or even melt ("core melt accidents").

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

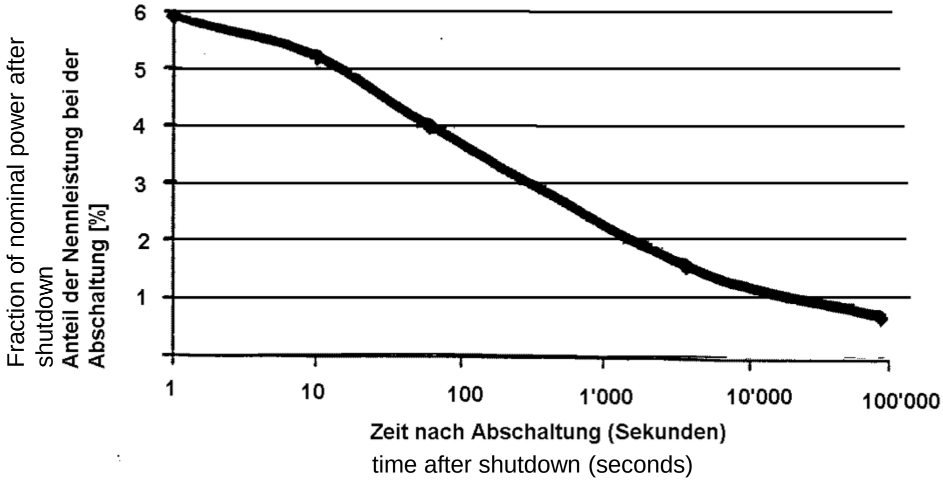
Laboratory for Safety Analysis
INSTITUTE FOR ENERGY TECHNOLOGY

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

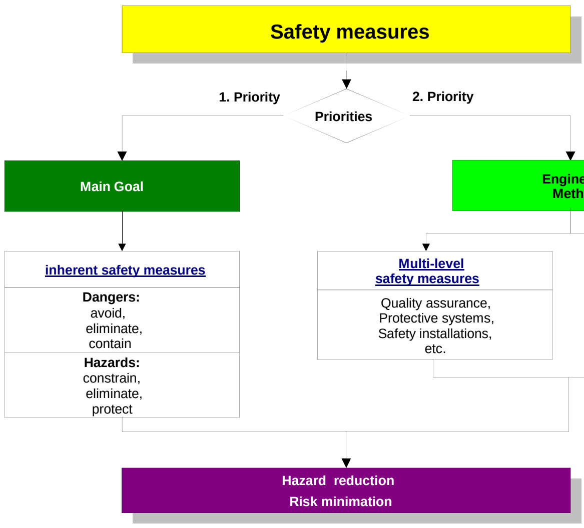
Reduction of the Radioactivity (Bq) of the Fission Products after Reactor Shutdown



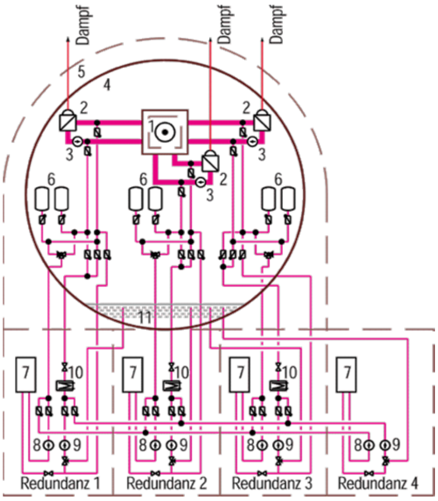
Decay Heat after Shutdown of the Reactor



Safety-Oriented Approach as Basis for Risk Management

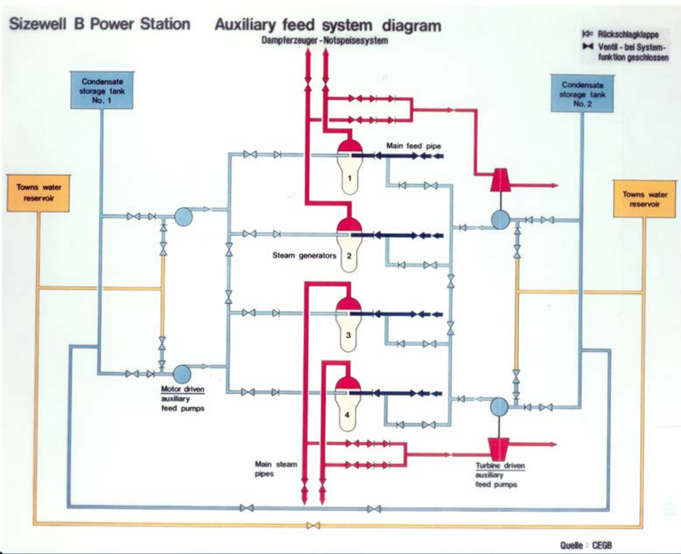


Emergency Core Cooling Systems (NPP Gösgen) – Redundancy as main principle



1. Reactor
2. Steam generator
3. Main cooling water pumps
4. Containment
5. Reactor building
6. Accumulators
7. Flooding water tank
8. Safety injection pumps (high pressure)
9. Residual heat cooling pumps (low pressure)
10. Residual heat cooler
11. Containment sump

Optimised design based on redundancy and diversity



Safety Features of Nuclear Power Plants

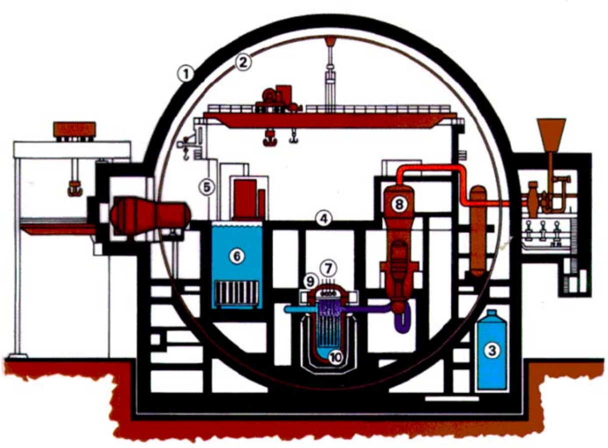
The major engineering safety features to cope with LOCA:

1. The Emergency Core Cooling System (ECCS) designed to supply water to the reactor core in the event of a Loss of Coolant Accident (LOCA).
2. The containment vessel, which is designed to provide a barrier to the escape to the environment of possible radioactivity released in the event of an accident.
3. The clean-up system designed to remove part of the radioactivity and the heat that may be present in the containment.
4. Hydrogen control to prevent formulation of an explosive Hydrogen-Oxygen mixture in the containment.

The Emergency Core Cooling System of a pressurised water reactor consists of:

1. High Pressure Injection System (HPIS)
2. Accumulator Injection System, Low Pressure Injection System (LPIS, active system)

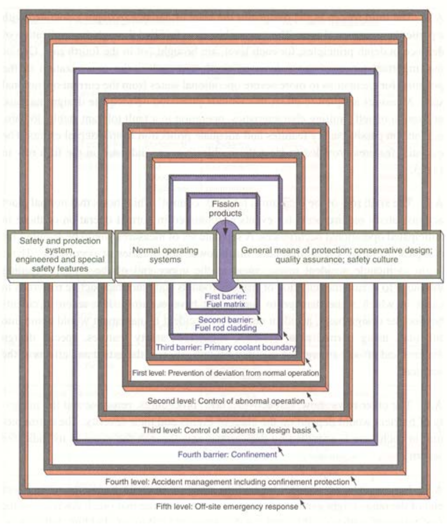
Containment of a Pressurised Water Reactor



Design values of a KWU KONVOI plant containment

Pressure: 5.3 bar
Temperature: 145˚ C
Leakage rate: 0.25 weight-%/d
Accessible during normal operation

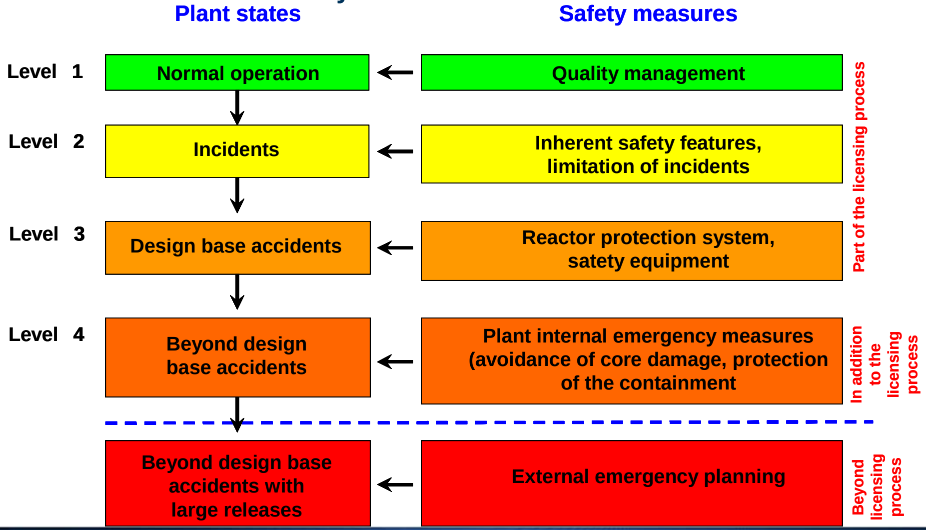
Concept of Multiple Levels of Protection ("Defence-in-Depth")



Physical Barriers of a Light Water Reactor

- **Fuel matrix** (made of ceramic material, which has a lower heat flux conductivity compared to metallic uranium, but a higher melting point).
- **Fuel rod** (made of zircaloy used for reasons of the neutron flux) keeps mechanically together the fuel pellets and retains fission products.
- **Envelop of primary loop** (in case of PWR: reactor pressure vessel and pipes to and within the steam generator; in case of BWR also the water-steam-circuit including the turbine housing; made of high quality steal).
- **Containment** designed against pressures in case of accidents and for the reactor protection against external loads; adequate sub-systems for the complete isolation against the environment.

Possible States of a Nuclear Installation Corresponding Protection Levels and Related Safety Measures



Design Basis Accidents (DBA)

- Selection of (representative, covering) accidents, which are expected to occur during the lifetime of a nuclear power plant or which cannot be excluded following human discretion (i.e. frequency > 10^{-6} per year).
- Design of the plant in such a manner, that the occurrence of such an accident does not lead to unacceptable consequences in the environment.
- For the verification, both an accident initiating event and the unavailability of an independent safety system needed to handle accidents are assumed (redundancy criterion; there is no need to assume additional system failures).

Beyond Design Basis Accidents (BDBA)

- Accidents are beyond design basis, if they can be characterised by multiple failures of systems needed to handle accidents or if they are instantiated by very rare events. The occurrence of such accidents is understood, based on the experience, as very unlikely (frequency < 10^{-6} per year).
- In contrast to DBA, it cannot be excluded that radioactive substances in a harmful amount are released to the environment; no dose limits for persons around the site are defined.

Safety Concept According to Swiss HSK-R-100[1)]

Safety level	Category	Frequency H per year	Verification	Goal	Dose limit environment	Dose limit workers
Normal operation						
Incidents		$H>10^{-1}$	Covered by deterministic accident analysis	Prevention of incidents and accidents, minimisation of radiation to workers	Q-DRW	20 mSv/year
Design base accidents	1	$10^{-2}H<10^{-1}$	Deterministic accident analysis, safety systems are available as required	Prevention of damage to: - safety relevant components - fuel clading	Q-DRW	50 mSv 250 mSv
	2	$10^{-4}<H<10^{-2}$		Limitation of damage to: - safety relevant components - fuel clading	1 mSv	50 mSv 250 mSv
	3	$10^{-6}<H<10^{-4}$		Assuring the - coolability of the reactor core - integrity of the containment	100 mSv	50 mSv 250 mSv
Beyond design base accidents		$H<10^{-6}$	PSA	Limitation of the consequences by including the radioactivity or the controlled release of radioactivity into the environment (internal accident management)	-	50 mSv 250 mSv
			Emergency preparedness	Mitigation of radiological consequences in the environment (external accident management)	-	50 mSv 250 mSv

[1)] 12/2004, replaced by SR 732.112.2 and ENSI-A01

Safety Concept

(Swiss Ordinance Protection against accidents in nuclear facilities, SR 732.112.2, 6/2009)

Basic provisions

Design Basis Accidents

- Categories:
  1. $\leq 10^{-1} \ldots > 10^{-2}$
  2. $\leq 10^{-2} \ldots > 10^{-4}$
  3. $\leq 10^{-4} \ldots > 10^{-6}$
- No ineligible release of radio activity and radiation of persons, limits – depending on frequency of DBA – fixed by radiation protection ordinance
- Frequency to be determined by multiplication of frequency of initiating event and single failure probability (0.1, 0.01 if proven by experience)

Beyond Design Basis Accidents

- Initiating events and additional failures beyond design
- Release of dangerous amounts of rad. substances cannot be excluded

Concept of defense in depth

Protection Goals

- control of reactivity
- cooling of core material and rad. waste
- confinement of rad. substances
- limitation of radiation expose

Accident Analysis

- deterministic analysis to demonstrate compliance with protective goals
- probabilistic analysis (PSA) to demonstrate that protective measures are sufficient and balanced.

Target values for existing NPPs

- total core damage frequency (CDF) less than 10^{-4}/a
- adequate precautions against accidents for CDF between 10^{-4} and 10^{-5}/a
- frequency of large release of rad. substances significantly less than CDF
- Guidelines for PSA - requirements to be established
- proof of sufficient protection against natural events for hazards $\geq 10^{-4}$/a, e.g. earthquakes
- protection against aircraft crash for military and commercial planes in operation when applying for a construction license

Design Basis Accidents according to Swiss ENSI-A01, 4.2.1c (7/2009)

- Heat removal from the reactor primary circuit
  - Loss of offsite power
  - Main reactor coolant pump failure
  - Inadvertent opening / stuck open Safety Relief Valves (SRV)
  - Inadvertent closure of all Main Steam Isolation Valves (MSIV)
  - 2F main steam line break inside and outside the primary containment
  - 2F feedwater line break inside and outside the primary containment
- Reactivity addition
  - Inadvertent control rod withdrawal
  - Spurious control rod ejection
- Loss of reactor coolant accident (LOCA)
  - 2F main reactor coolant pipe
  - Breaks and leaks in the main reactor coolant system
  - Breaks and leaks in the reactor coolant sampling and measuring lines outside the primary containment
  - 2F steam generator tube rupture

Design and Construction of Nuclear Installations

- The design of nuclear power plants allows withstanding a set of events and resulting loads in an acceptable way.
- Classification of different events based on their frequency of occurrence; events covering all incidents used as design base (e.g. guillotine break of the main cooling pipe); fulfilling deterministically safety and protection goals (e.g. 3 × 100% or 4 × 50% redundant design of vital safety systems).
- Accident scenarios with an extreme low probability of occurrence are investigated within a probabilistic risk analysis (PRA).
- Design limits are not fixed but flexible based on experience gained and development of state of science and technology and related safety requirements.
- Experience from operation and incidents within the design base, data collected and evaluated in order to avoid repetition of unwanted events (e.g. OECD/NEA – IAEA IRS).
- Standardisation as natural development, implementation with delay.

Future Requirements

Commonly shared principles for all types of nuclear power plants and for all countries:

"to prevent with high confidence accidents in nuclear plants; to ensure that, for all accidents taken into account in the design of the plant, even those of very low probability, radiological consequences, if any, would be minor; and to ensure that the likelihood of severe accidents with serious radiological consequences is extremely small."

Source: INSAG - 12

- **EPR safety objectives, motivated by the continuous search for a higher safety level, involve reinforced application of the defence-in-depth concept:**
- by improving the preventive measures in order to further reduce the probability of core melt, and
- by simultaneously incorporating, right from the design stage, measures for limiting the consequences of a severe accident.

Comparison of “Users Requirements” for Future Reactor Concepts

	EPRI “Utility’s Requirements“	„European Utility Requirements“ (EUR)
	Simple, rugged, high design margin, based on proven technology	Evolutionary PWR, 1000-1500 MWe; evolutionary BWR and small LWR with passive features as „acceptable competitors“
Safety	Protection of society, workers and investment. Accident resistance: • Core damage frequency < 10-5 per reactor year • Station blackout coping time for core cooling: 8 hours minimum • No operator action for at least 72 hours needed (only „advanced passive“)	Accident resistance: • Core damage frequency < 10^{-5} per reactor year • Release frequencies for severe accidents [10^{12} Bq]:

	short term < 24 h	long term
Xe_{133}	10^5	10^6
I_{131}	300	2000
Cs_{137}	-	100

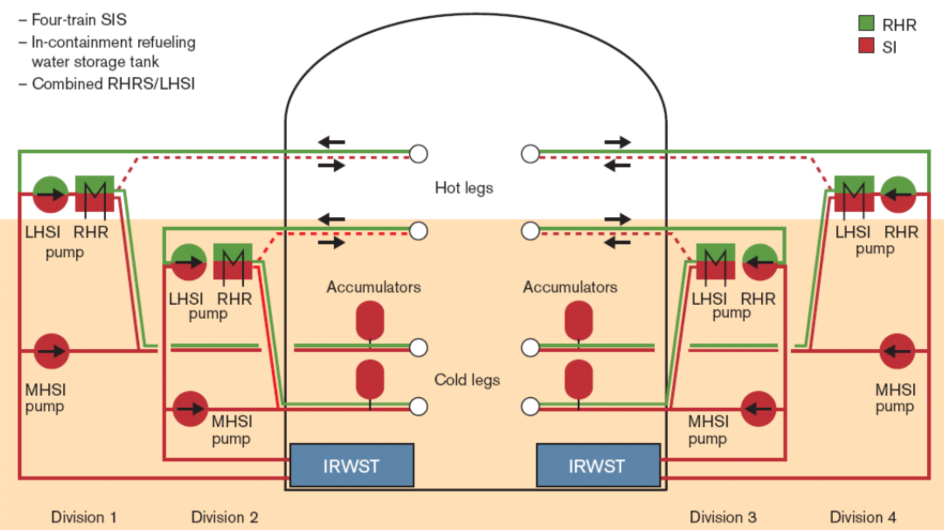
Comparison of "Users Requirements" for Future Reactor Concepts (cont.)

	Accident mitigation: • Dose < 0.25 Sv at the site boundary for severe accidents with cumulative frequency > 10-6 per year	Accident mitigation: • Probability of large releases < 10-6 per reactor year
Performance	Long plant design life (60 a), high availability (87%)	Long plant design life (40 a) without refurbishment, high availability (87%).
Economics	10-20% cost advantage over alternatives	15% cost advantage over alternatives (coal, combined cycle)

IAEA target values for core damage frequency (CDF)
- for existing plants: 10^{-4} per reactor-year
- for future plants: 10^{-5} per reactor-year

EPR Safety Injection / Residual Heat Removal (SIS/RHRS)

- Four-train SIS
- In-containment refueling water storage tank
- Combined RHRS/LHSI



EPR Containment Heat Removal System