Design Requirements – Safety and Critical Safety Functions

22.39 Elements of Reactor Design, Operations, and Safety

Lecture 6

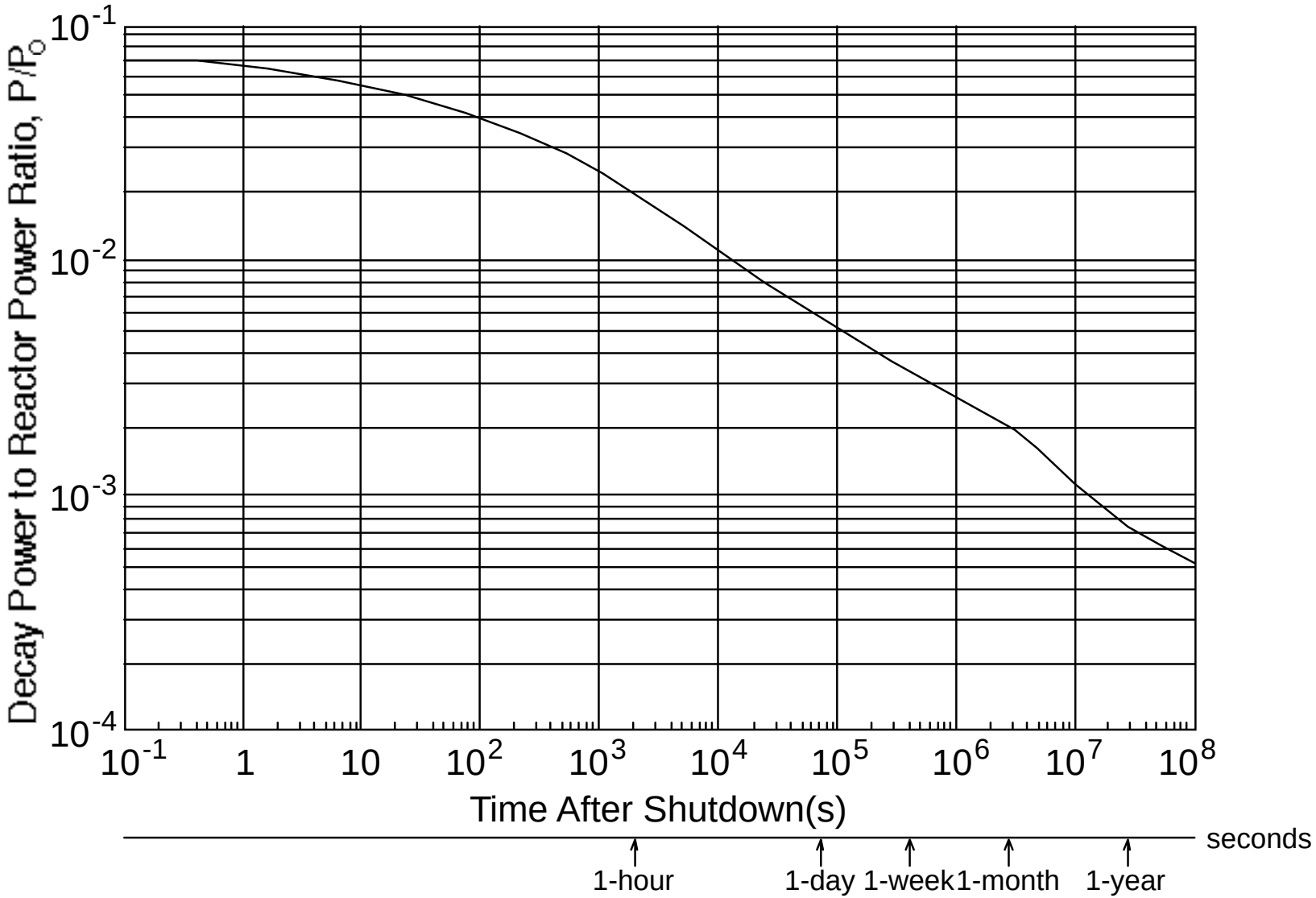
Fall 2006

George E. Apostolakis
Massachusetts Institute of Technology

The Hazard (some fission-product isotopes)

Isotope	Half-Life	Volatility	Health Hazard
^{131}I	8 d	Gaseous	External whole-body radiation; internal irradiation of thyroid; high toxicity
^{89}Sr	54 y	Moderately volatile	Bones and lungs
^{106}Ru	1 y	Highly volatile	Kidneys
^{137}Cs	33 y	Highly volatile	Internal hazard to whole body

Decay Heat



Source: Todreas & Kazimi, Vol. 1

CRITICAL SAFETY FUNCTIONS
HARDWARE / TRAINING / PROCEDURES / CULTURE

KEEP FISSION PRODUCTS WITHIN THE FUEL

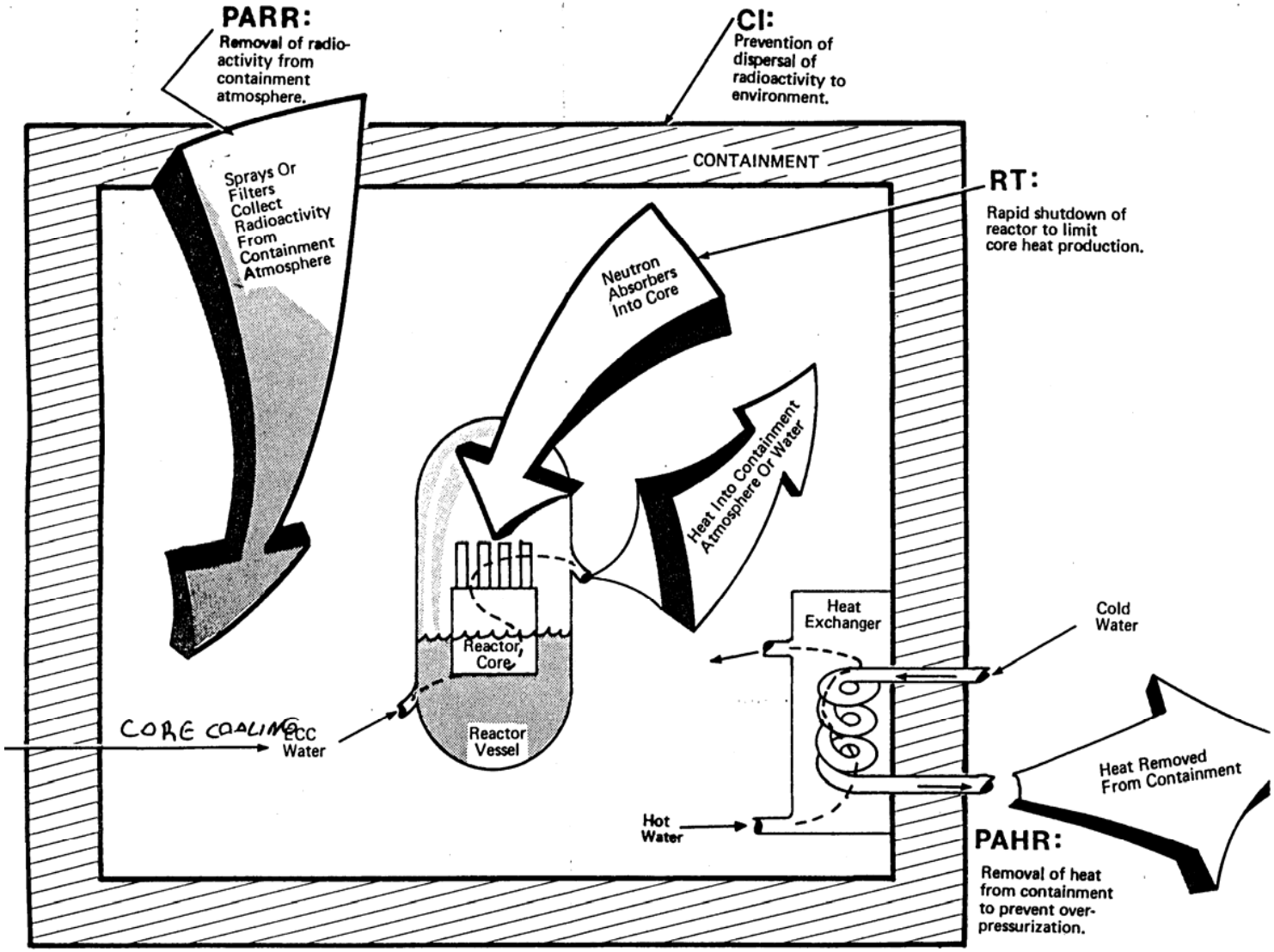
- Control Reactor Power
  - Control reactivity additions
  - Shutdown reliably
- Cool the Reactor and Spent Fuel
  - Maintain coolant inventory
  - Maintain coolant flow
  - Maintain coolant heat sinks

KEEP RADIOACTIVE MATERIAL OUT OF THE BIOSPHERE

- Maintain Containment Integrity
  - Prevent over-pressurization
  - Prevent over-heating
  - Prevent containment bypass
- Capture Material Within Containment
  - Scrubbing
  - Deposition
  - Chemical capture

SHIELD PERSONNEL FROM RADIATION

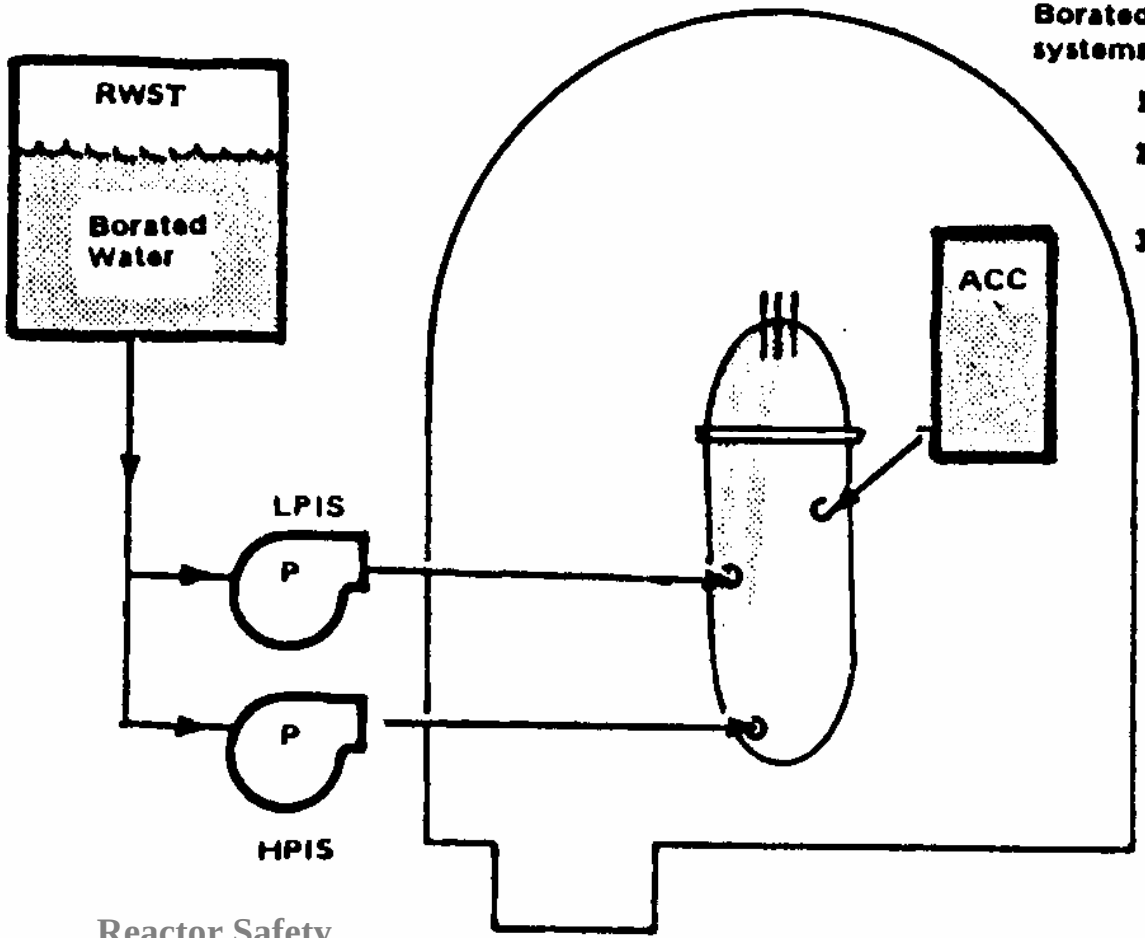
Emergency Safety Functions



Reactor Safety Study, WASH-1400

(U.S. Atomic Energy Agency)

PWR SYSTEMS USED TO PERFORM EMERGENCY FUNCTIONS: ECI



ECI

Borated water is furnished to cool the core by three systems:

1) Accumulators,
2) the Low Pressure Injection System (LPIS), and
3) the High Pressure Injection System (HPIS).

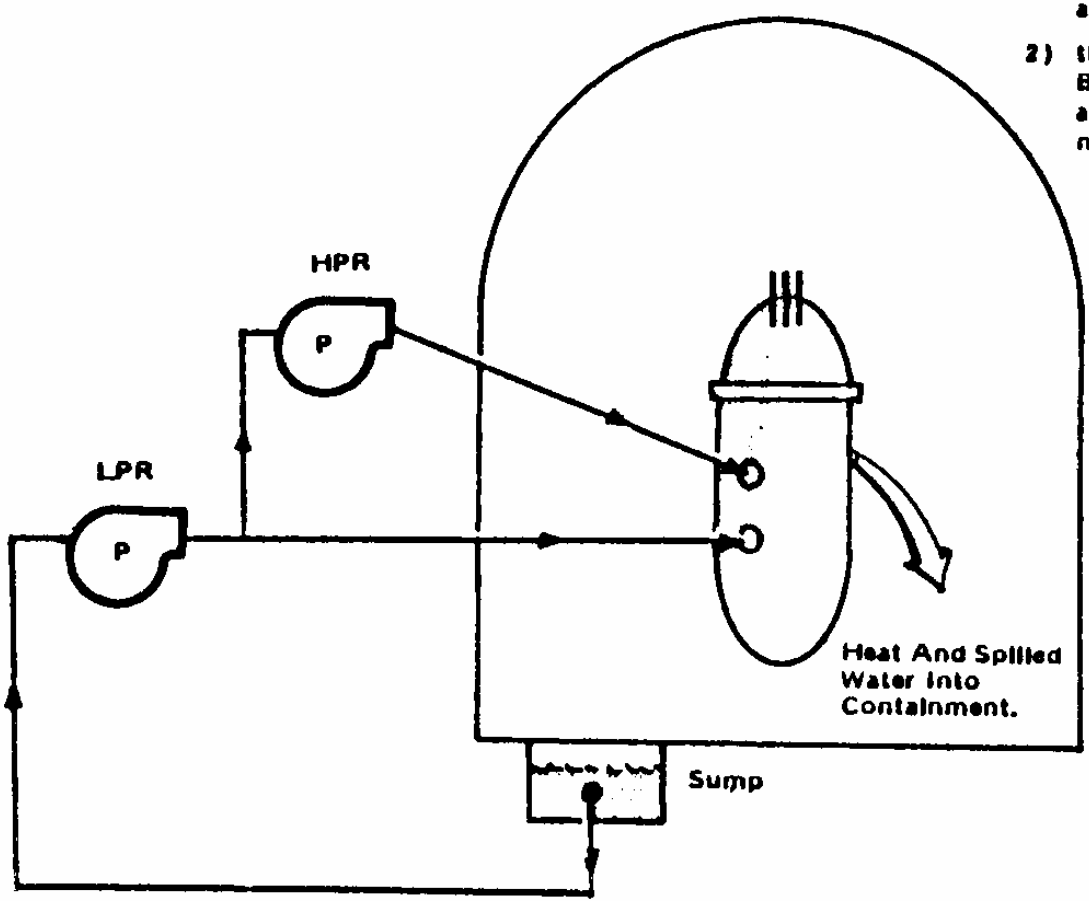
Reactor Safety Study, WASH-1400

PWR SYSTEMS USED TO PERFORM EMERGENCY FUNCTIONS: ECR

ECR

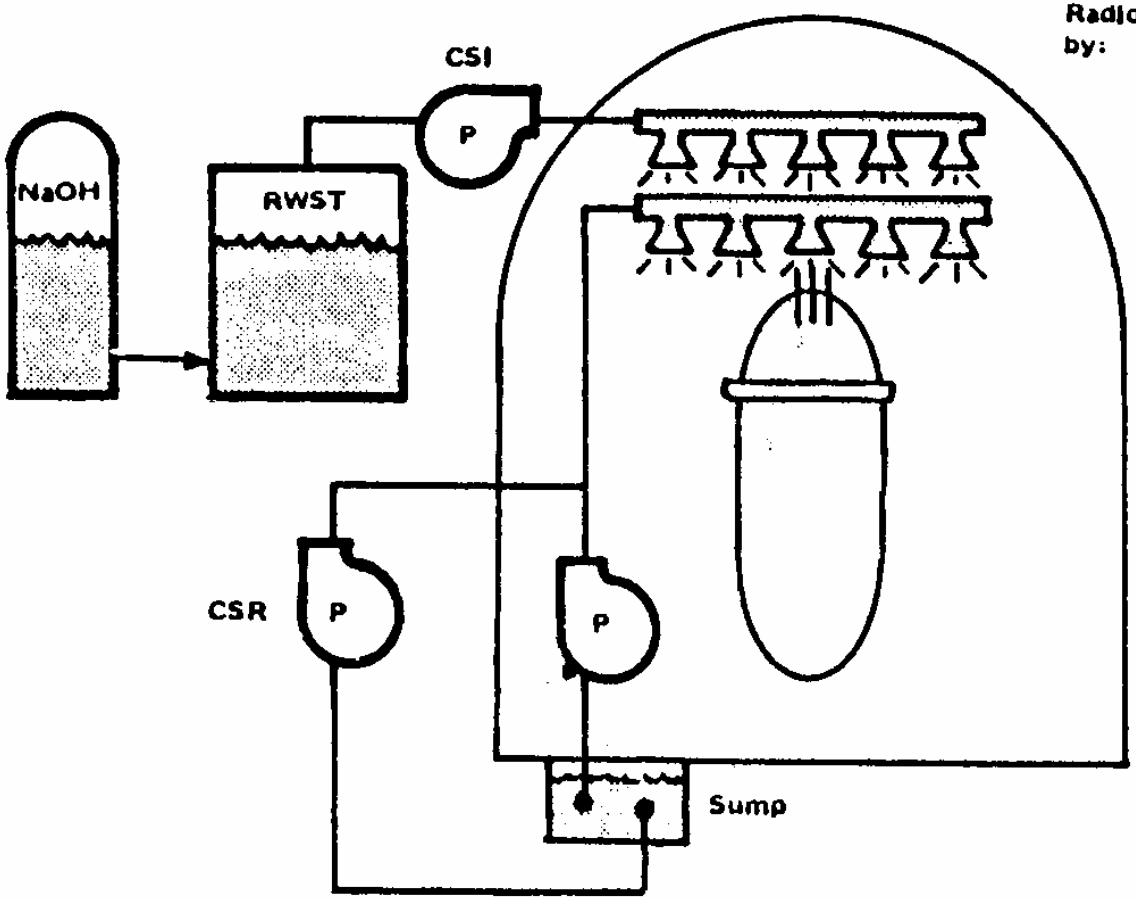
The core is cooled by heat being transferred to containment by two systems:

1) the Low Pressure Recirculation System (LPRS), and
2) the High Pressure Recirculation System (HPRS). Both systems, using injection pumps aligned to a recirculation mode, pump water from a containment sump into the core.



Reactor Safety Study, WASH-1400

PWR SYSTEMS USED TO PERFORM EMERGENCY FUNCTIONS: PARR



PARR

Radioactivity is collected from the containment atmosphere by:

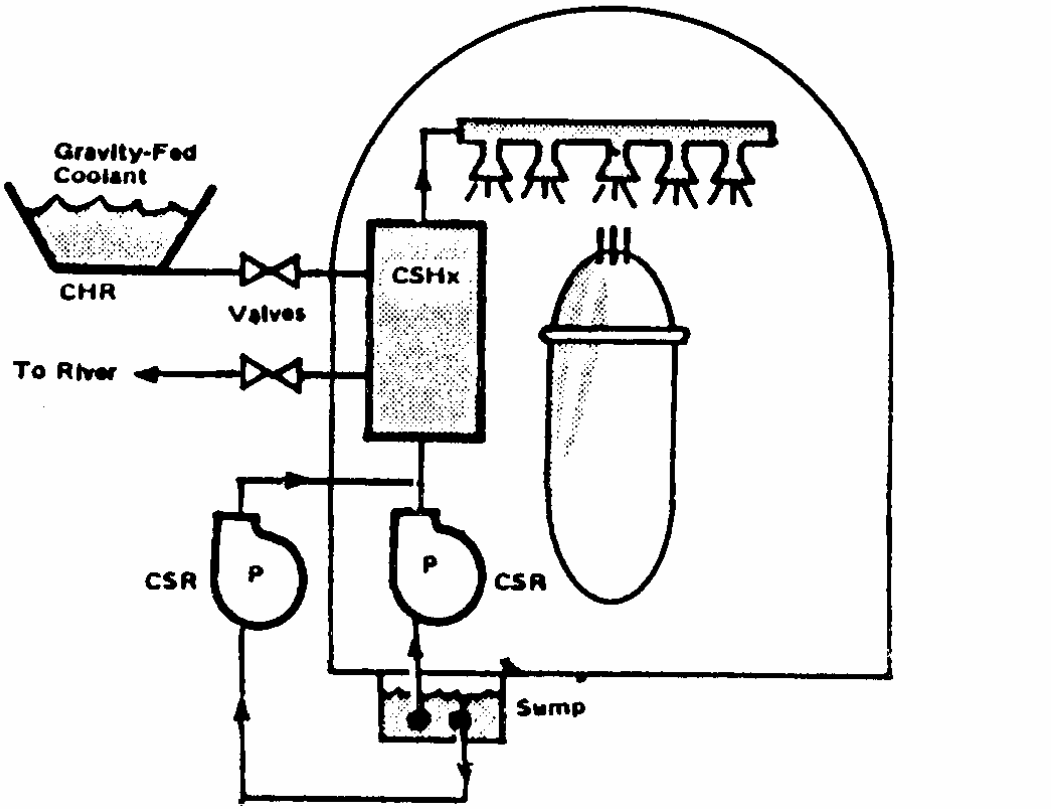
1) the Containment Spray Injection System (CSIS),
2) the Containment Spray Recirculation System (CSRS), and
3) Sodium Hydroxide Addition (SHA) to spray water.

PWR SYSTEMS USED TO PERFORM EMERGENCY FUNCTIONS: PAHR

PAHR

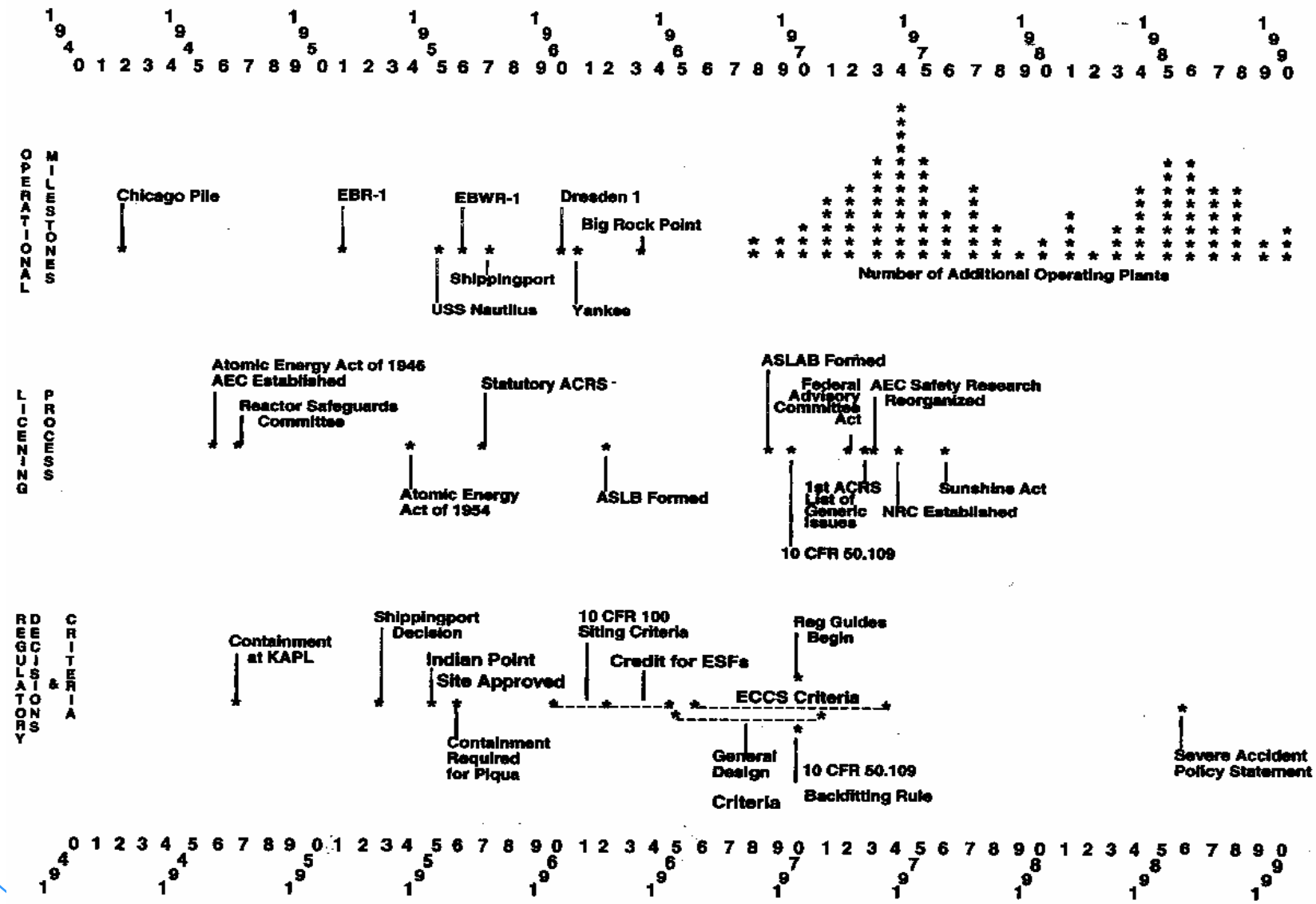
Heat is removed from containment by heat exchangers that involve two systems:

1) the Containment Spray Recirculation System, and
2) the Containment Heat Removal System (CHRS).

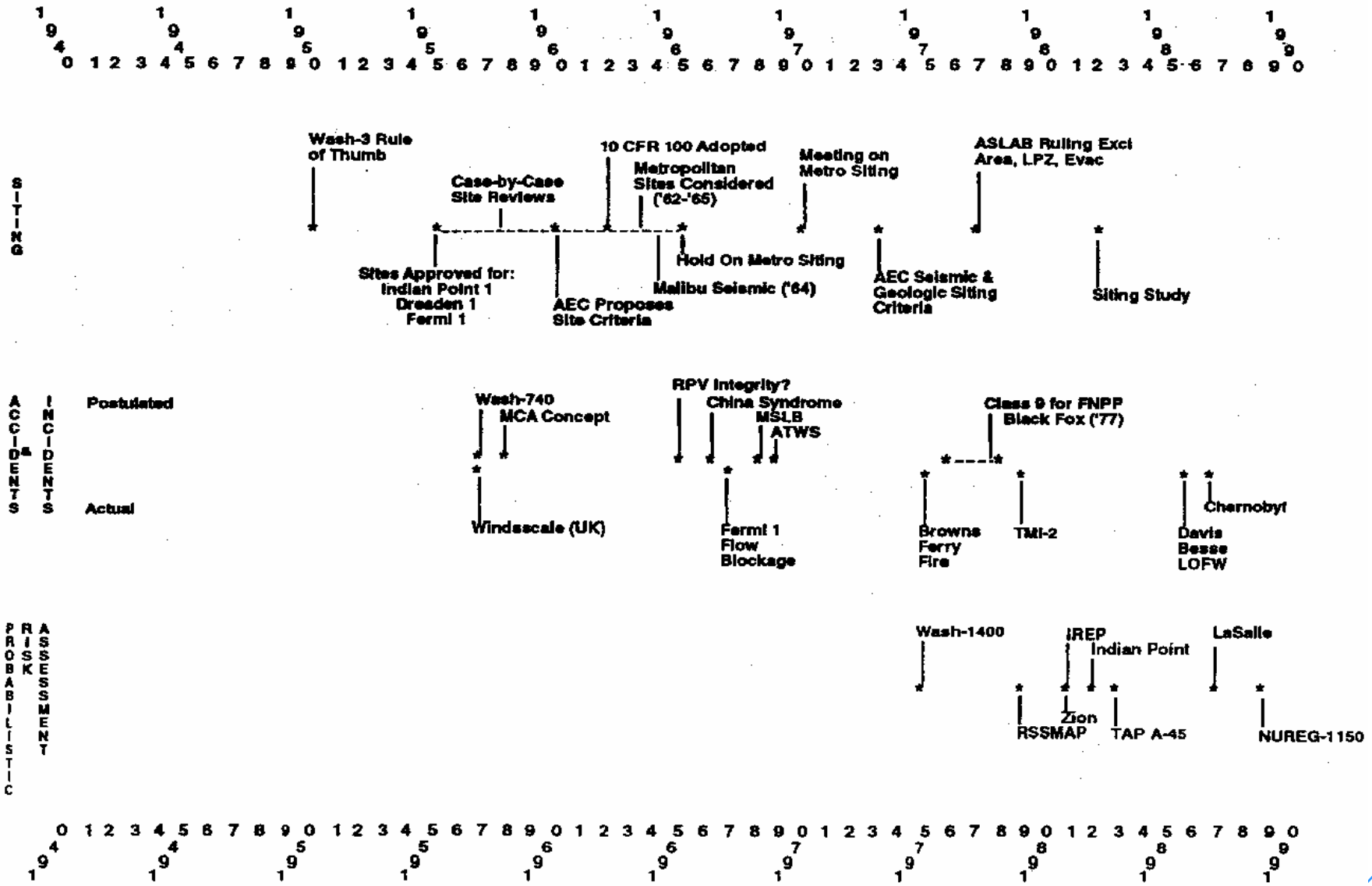


Reactor Safety Study, WASH-1400

TIMING OF MAJOR EVENTS FROM 1940s TO PRESENT (1 of 2), NUREG/CR-6042, 1994



TIMING OF MAJOR EVENTS FROM 1940s TO PRESENT (2 of 2)), NUREG/CR-6042, 1994



Siting Criteria (10 CFR 100)

- **Consideration of:**
  - **Characteristics of reactor design**
  - **Population characteristics, exclusion area, low population zone, population center distance**
    - ✓ **Assume a bounding fission product release based on a major accident**
    - ✓ **Define an exclusion area of such size that an individual located at any point on its boundary for two hours immediately following the accident would not receive a total radiation dose to the whole body in excess of 25 rem (250 mSv) or a total radiation dose in excess of 300 rem (3000 mSv) to the thyroid from iodine exposure.**
    - ✓ **Define a low population zone of such size that an individual located at any point on its outer boundary who is exposed to the radioactive cloud during the entire period of its passage would not receive a total radiation dose to the whole body in excess of 25 rem (250 mSv) or a total radiation dose in excess of 300 rem (3000 mSv) to the thyroid from iodine exposure.**
    - ✓ **A population center distance of at least 1.33 times the distance from the reactor to the outer boundary of the population center distance**
  - **Seismology, meteorology, geology, hydrology.**

General Design Criteria (10 CFR 50 Appendix A)

http://www.nrc.gov/reading-rm/doc-collections/cfr/part050/

- **The principal design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety; that is, structures, systems, and components that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.**

- **Six major categories:**
  - **Overall requirements**
  - **Protection by multiple fission product barriers**
  - **Protection and reactivity control systems**
  - **Fluid systems**
  - **Reactor containment**
  - **Fuel and reactivity control**

The Single-Failure Criterion

- **"Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions."**

- **The intent is to achieve high reliability (probability of success) without quantifying it.**

- **Looking for the worst possible single failure leads to better system understanding.**

GDC 10 and 11

- ***Criterion 10--Reactor design*. The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.**

- ***Criterion 11--Reactor inherent protection*. The reactor core and associated coolant systems shall be designed so that in the power operating range the net effect of the prompt inherent nuclear feedback characteristics tends to compensate for a rapid increase in reactivity.**

GDC 35

- **An ECCS must be designed to withstand the following postulated LOCA: a double-ended break of the largest reactor coolant line, the concurrent loss of offsite power, and a single failure of an active ECCS component in the worst possible place.**

Defense in Depth

"Defense-in-Depth is an element of the Nuclear Regulatory Commission's safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility."

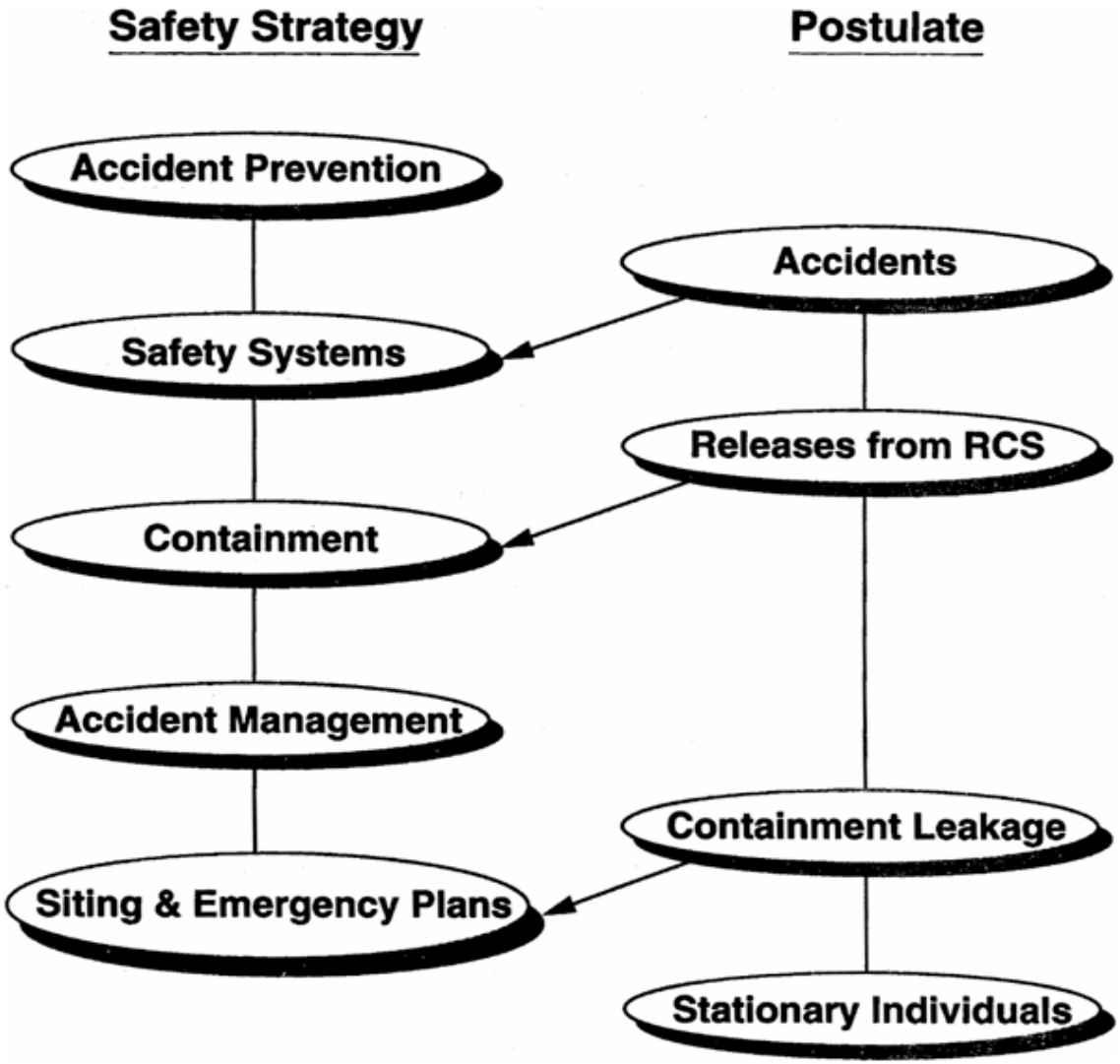
[Commission's White Paper, USNRC, 1999]

DEFENSE-IN-DEPTH MULTILAYER PROTECTION FROM FISSION PRODUCTS

Barrier or Layer	Function
1. Ceramic fuel pellets	Only a fraction of the gaseous and volatile fission products is released from the pellets.
2. Metal cladding	The cladding tubes contain the fission products released from the pellets. During the life of the fuel, less than 0.5 percent of the tubes may develop pinhole sized leaks through which some fission products escape.
3. Reactor vessel and piping	The 8- to 10-inch (20- to 25-cm) thick steel vessel and 3- to 4-inch (7.6- to 10.2-cm) thick steel piping contain the reactor cooling water. A portion of the circulating water is continuously passed through filters to keep the radioactivity low.
4. Containment	The nuclear steam supply system is enclosed in a containment building strong enough to withstand the rupture of any pipe in the reactor coolant system.
5. Exclusion area	A designated area around each plant separates the plant from the public. Entrance is restricted.
6. Low population zone, evacuation plan	Residents in the low population zone are protected by emergency evacuation plans.
7. Population center distance	Plants are located at a distance from population centers.

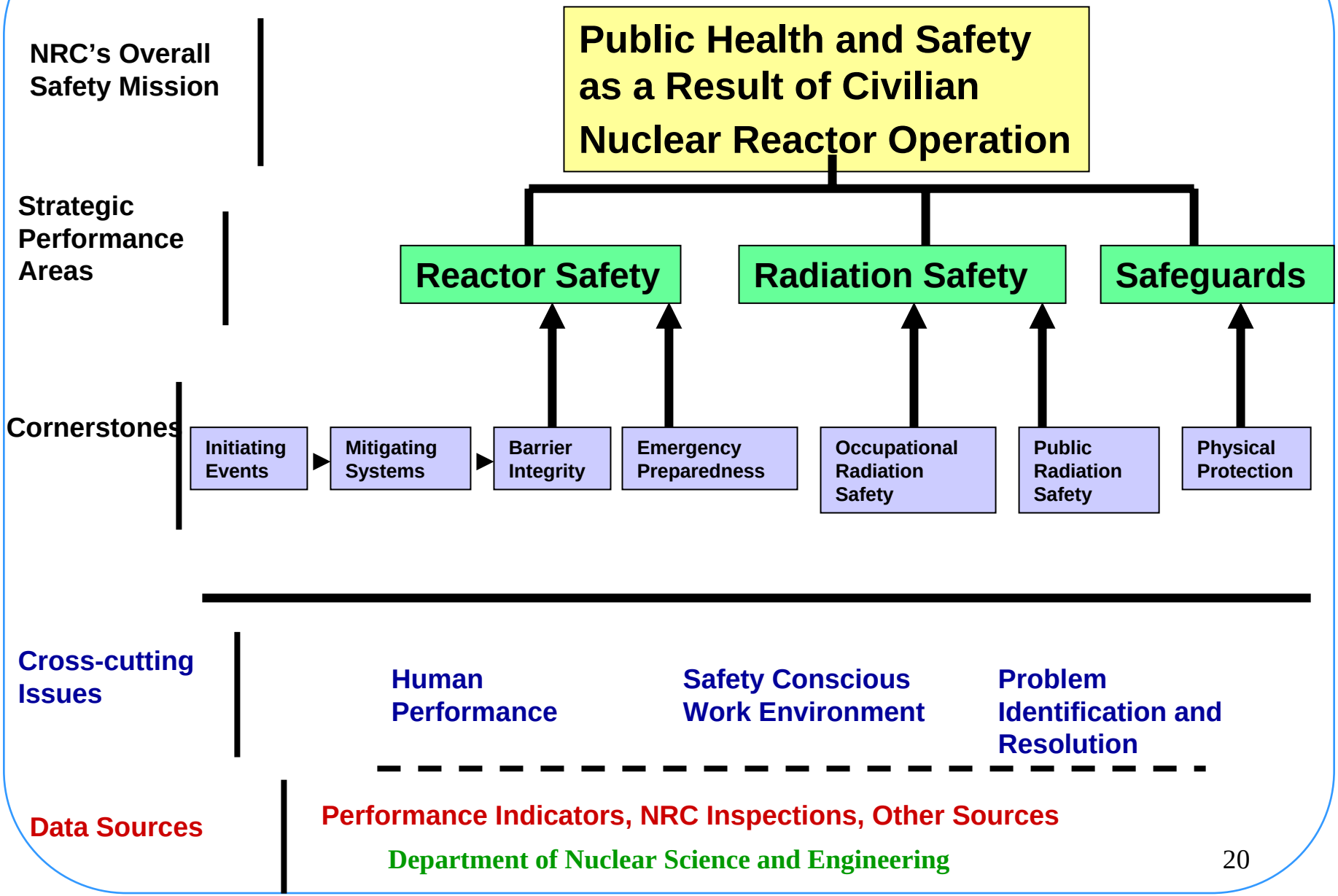
NUREG/CR-6042, 1994.

DEFENSE-IN-DEPTH, SAFETY STRATEGIES



NUREG/CR-6042, USNRC, 1994.

Reactor Oversight Process



CHAPTER TITLES FROM RG 1.70 REV. 3 STANDARD FORMAT AND CONTENT OF SAFETY ANALYSIS REPORTS FOR NUCLEAR POWER PLANTS

Chapter 1	**Introduction and General Description of Plant**
Chapter 2	**Site Characteristics**
Chapter 3	**Design of Structures, Components, Equipment, and Systems**
Chapter 4	**Reactor**
Chapter 5	**Reactor Coolant Systems and Connected Systems**
Chapter 6	**Engineered Safety Features**
Chapter 7	**Instrumentation and Controls**
Chapter 8	**Electric Power**
Chapter 9	**Auxiliary Systems**
Chapter 10	**Steam and Power Conversion System**
Chapter 11	**Radioactive Waste Management**
Chapter 12	**Radiation Protection**
Chapter 13	**Conduct of Operations**
Chapter 14	**Initial Test Program**
Chapter 15	**Accident Analysis**
Chapter 16	**Technical Specifications**
Chapter 17	**Quality Assurance**

NUREG/CR-6042, USNRC, 1994.

Design Basis Accidents

- **A DBA is a postulated accident that a facility is designed and built to withstand without exceeding the offsite exposure guidelines of the NRC's siting regulation (10 CFR Part 100).**

- **Each DBA includes at least one significant failure of a component. In general, failures beyond those consistent with the single-failure criterion are not required (unlike in PRAs).**

NUREG/CR-6042, USNRC, 1994.

REACTOR FACILITY CLASSIFICATION OF POSTULATED ACCIDENTS AND OCCURRENCES

Class Number	Description	Example(s)
1	Trivial incidents	Small spills Small leaks inside containment
2	Miscellaneous small releases outside containment	Spills Leaks and pipe breaks
3	Radwaste system failures	Equipment failure Serious malfunction or human error
4	Events that release radioactivity into the primary system	Fuel defects during normal operation Transients outside expected range of variables
5	Events that release radioactivity into the secondary system	Class 4 and heat exchanger leak
6	Refueling accidents inside containment	Drop fuel element Drop heavy object onto fuel Mechanical malfunction or loss of cooling in transfer tube
7	Accidents to spent fuel outside containment	Drop fuel element Drop heavy object onto fuel Drop shielding cask—loss of cooling to cask, transportation incident on site
8	Accident initiation events considered in design basis evaluation in the safety analysis report	Reactivity transient Rupture of primary piping Flow decrease—steamline break
9	Hypothetical sequences of failures more severe than Class 8	Successive failures of multiple barriers normally provided and maintained

U.S. Atomic Energy Commission, 1973.

REPRESENTATIVE INITIATING EVENTS TO BE ANALYZED IN SECTION 15.X.X OF THE SAR

1. Increase in Heat Removal by the Secondary System

1.1 Feedwater system malfunctions that results in a decrease in feedwater temperature.
1.2 Feedwater system malfunctions that result in an increase in feedwater flow.
1.3 Steam pressure regulator malfunction or failure that results in increasing steam flow.
1.4 Inadvertent opening of a steam generator relief or safety valve.
1.5 Spectrum of steam system piping failures inside and outside of containment in a PWR.

2. Decrease in Heat Removal by the Secondary System

2.1 Steam pressures regulator malfunction or failure that results in decreasing steam flow.
2.2 Loss of external electric load.
2.3 Turbine trip (stop valve closure).
2.4 Inadvertent closure of main steam isolation valves.
2.5 Loss of condenser vacuum.
2.6 Coincident loss of onsite and external (offsite) a.c. power to the station.
2.7 Loss of normal feedwater flow.
2.8 Feedwater piping break.

3. Decrease in Reactor Coolant System Flow Rate

3.1 Single and multiple reactor coolant pump trips.
3.2 BWR recirculation loop controller malfunctions that result in decreasing flow rate.
3.3 Reactor coolant pump shaft seizure.
3.4 Reactor coolant pump shaft break.

NUREG/CR-6042, USNRC, 1994.

REPRESENTATIVE INITIATING EVENTS TO BE ANALYZED IN SECTION 15.X.X OF THE SAR (cont.)

4. Reactivity and Power Distribution Anomalies

4.1 Uncontrolled control rod assembly withdraws from a subcritical or low power startup condition (assuming the most unfavorable reactivity conditions of the core and reactor coolant system), including control rod or temporary control device removal error during refueling.

4.2 Uncontrolled control rod assembly withdraws at the particular power level (assuming the most unfavorable reactivity conditions of the core and reactor coolant system) that yields the most severe results (low power to full power).

4.3 Control rod maloperation (system malfunction or operator error), including maloperation of part length control rods.

4.4 A malfunction or failure of the flow controller in BWR loop that results in an incorrect temperature.

4.5 A malfunction or failure of the flow controller in BWR loop that results in an increased reactor coolant flow rate.

4.6 Chemical and volume control system malfunction that results in a decrease in the boron concentration in the reactor coolant of a PWR.

4.7 Inadvertent loading and operation of a fuel assembly in an improper position.

4.8 Spectrum of rod ejection accidents in a PWR.

4.9 Spectrum of rod drop accidents in a BWR.

5. Increase in Reactor Coolant Inventory

5.1 Inadvertent operation of ECCS during power operations.

5.2 Chemical and volume control system malfunction (or operator error) that increases reactor coolant inventory

5.3 A number of BWR transients, including items 2.1 through 2.6 and item 1.2.

NUREG/CR-6042, USNRC, 1994.

REPRESENTATIVE INITIATING EVENTS TO BE ANALYZED IN SECTION 15.X.X OF THE SAR (cont.)

6. Decrease in Reactor Coolant Inventory

6.1 Inadvertent opening of a pressurizer safety or relief valve in a PWR or a safety or relief valve in a BWR.

6.2 Break in instrument line or other lines from reactor coolant pressure boundary that penetrate containment.

6.3 Steam generator tube failure.

6.4 Spectrum of BWR steam system piping failures outside of containment.

6.5 Loss-of-coolant accidents resulting from the spectrum of postulated piping breaks within the reactor coolant pressure boundary, including steam line breaks inside of containment in a BWR.

6.6 A number of BWR transients, including items 2.7, 2.8, and 1.3.

7. Radioactive Release from a Subsystem or Component

7.1 Radioactive gas waste system leak or failure.

7.2 Radioactive liquid waste system leak or failure.

7.3 Postulated radioactive releases due to liquid tank failures.

7.4 Design basis fuel handling accidents in the containment and spent fuel storage buildings.

7.5 Spent fuel cask drop accidents.

NUREG/CR-6042, USNRC, 1994.

Emergency Core Cooling System (ECCS) (January 1974, 10 CFR 50.46)

- **Postulate several LOCAs of different sizes and locations to provide assurance that the most severe LOCAs are considered.**
- **Postulate concurrent loss of offsite or onsite power and the most damaging single failure of ECCS equipment (GDC 35).**
- **Acceptance Criteria**
  - **Peak cladding temperature cannot exceed 2200 ºF (1204 ºC)**
  - **Oxidation cannot exceed 17% of cladding thickness**
  - **Hydrogen generation from hot cladding-steam interaction cannot exceed 1% of its potential**
  - **Core geometry must be coolable**
  - **Long-term cooling must be provided**

Seismic Design Basis

- ***Operating Basis Earthquake (OBE)*: the largest EQ that could reasonably be expected to affect the plant site during the operating life of the plant and for which the plant is designed to continue operating without undue risk to the health and safety of the public.**

- ***Safe Shutdown Earthquake (SSE):* the maximum potential EQ considering local conditions and history. The plant may be damaged but it can be safely shut down.**

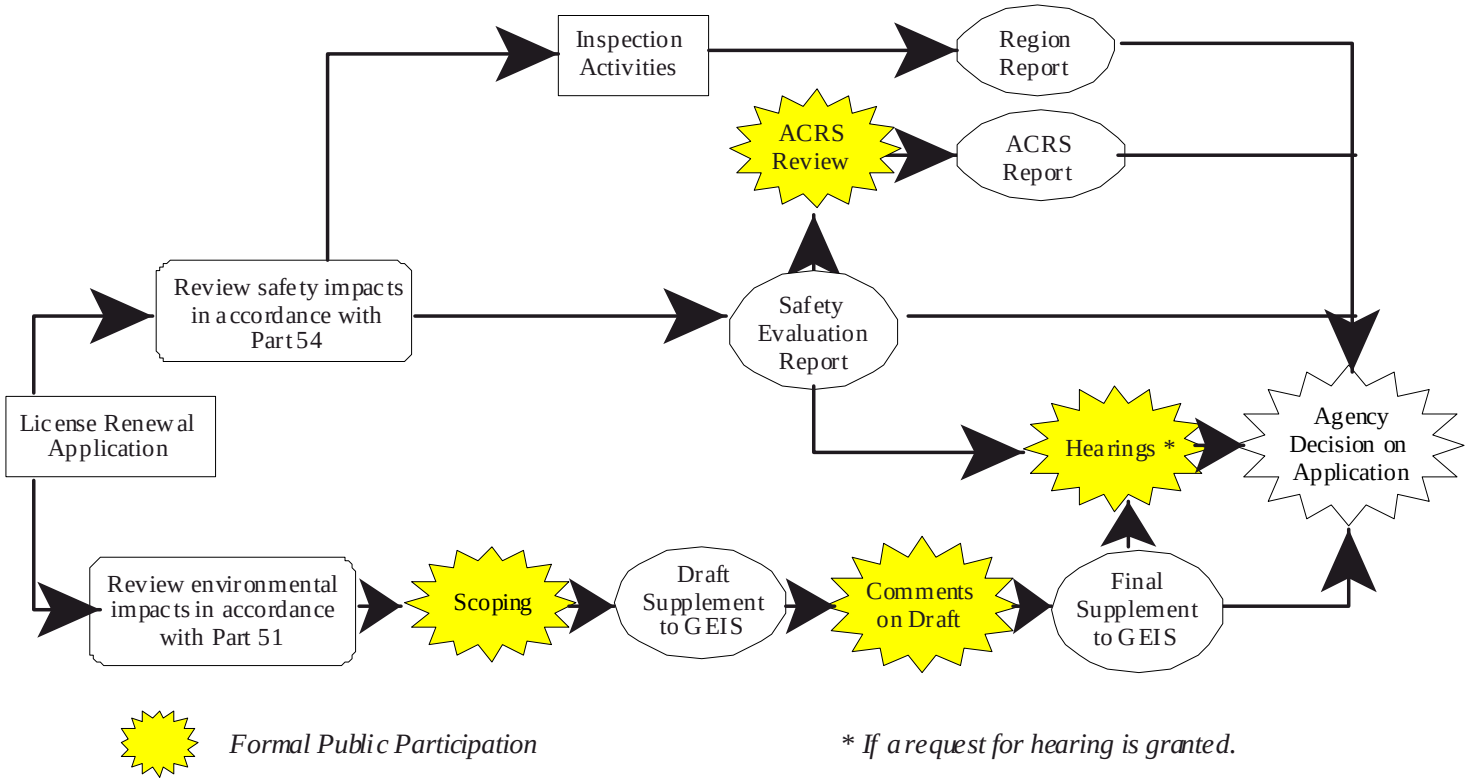
What is License Renewal?

- **Atomic Energy Act**
  - **40-year license to operate**
  - **Allows for renewal**
- **License will expire for four plants in 2009 and for an additional 25 plants by 2015.**
- **10 CFR Part 54 allows a new license to be issued to operate for up to 20 years beyond the current term**
- **Application submittal not earlier than 20 years before expiration of current license**

Principles of License Renewal

- **The regulatory process is adequate to ensure the safety of all currently operating plants, with the possible exception of the detrimental effects of aging on certain SSCs.**
- **10 CFR 54 focuses on managing the adverse effects of aging.**
- **Plant-specific licensing basis must be maintained during the renewal term in the same manner and to the same extent as during the original licensing term.**

Renewal Process



License Renewal Application (1)

- **Integrated plant safety assessment**
  - **Identify "passive" and "long-lived" SSCs important to safety, e.g., vessel, RCS piping, SGs, pump casings, valve bodies. (Aging effects on "active" SSCs are readily detected and corrected by existing programs.)**
  - **Describe and justify scoping and screening methodology**
  - **Demonstrate aging effects will be managed either by existing or new programs**

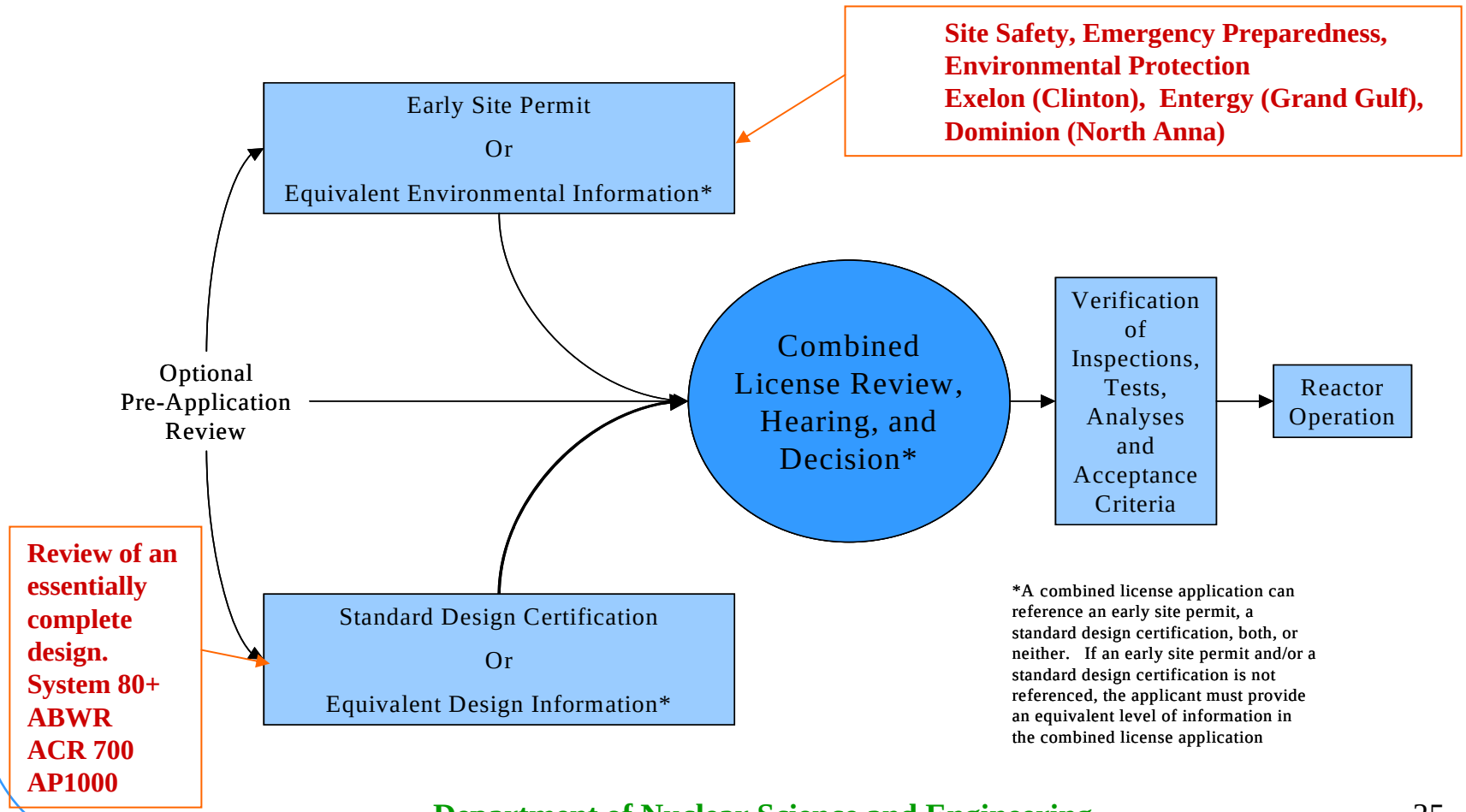
License Renewal Application (2)

- Evaluate time-limited aging analyses and exemptions (assumptions made during design of plant about its lifetime must be revisited and shown to be valid for extended operation)
- Final safety analysis report supplement
- Technical specification changes
- Environmental report

License Renewal Program Status

- **Renewed licenses issued for 26 units at 15 plants**
- **Applications for 18 units at 9 plants under review**
- **Applications for additional 8 units at 6 plants forecasted through 2005**

10 CFR Part 52
Future Licensing Process



Goals for Part 52 Process

- **Stable and predictable licensing process**
- **Resolve safety and environmental issues before authorizing construction**
- **Reduce financial risks to licensees (COL)**
- **Enhance safety and reliability through standardization of nuclear plant designs**