# Long-term Training Course
# on
# Safety Regulation and Safety Analysis / Inspection
# 2005

# OUTLINE OF SAFETY DESIGN
# (CASE OF BWR)

7 September – 11 November 2005
Tokyo, Japan

Japan Nuclear Energy Safety Organization

(JNES)

# Summary of Safety Design of Nuclear Power Station
(Case of BWR)

Contents

# 1. Concept of Safe Design of Nuclear Power Station

## 1.1 Three Principles of Safety Ensuring

Safety ensuring of nuclear power station is to prevent irradiation exposure to the public in the neighborhood of the nuclear power station.

The fundamental rules of safety ensuring are the following three principles, which are commonly called the three principles of safety ensuring.

- Reactor shutdown
- Reactor cooling
- Radiation confinement

### 1.1.1 Reactor shutdown

When any anomaly occurs during reactor operation, the reactor is shutdown to prevent further nuclear fission.

BWR is provided with two different systems to shutdown the reactor; one is the reactor shutdown system, which stops nuclear fission by inserting control rods into the reactor core. The control rods contain neutron absorbing materials. The other is the boron insertion system, which stops nuclear fission by injecting boric acid solution into the reactor core.

### 1.1.2 Reactor cooling

Even after the nuclear fission is stopped, the reactor releases decay heat from fission products in the core. Reactor cooling after shutdown is necessary, because the fuel assembly will be damaged by increasing in-core temperature, if the decay heat is not removed.

BWR is provided with a residual heat removal system, which consists of motor driven pumps and heat exchangers.

### 1.1.3 Radiation confinement

If radioactive materials leak from the core, the radioactivity must be confined to prevent outside leakage from the nuclear power station.

The radiation confinement is the ultimate means to protect the public in the neighborhood against radiation exposure. For this effect, the following 5 barriers are provided.

- Barrier 1. Fuel pellet matrix

The matrix itself of the fuel pellet, which is ceramic made of sintered $UO_2$ powder, has an excellent ability to retain fission products (FP) and, thus, the totality of the solid FP and most FP gases are contained in the matrix. The fuel temperature during operation is properly controlled to prevent FP from being melted and discharged outside.

- Barrier 2. Fuel cladding

Fuel cladding confines gaseous FP and is made to ensure its integrity by preventing damage due to the lack of coolant or interaction between fuel pellet and cladding.

At the occurrence of an accident involving a loss of coolant, ECCS will be activated to take over the cooling process and to prevent fuel from being damaged or melted.

- Barrier 3. Primary coolant pressure boundary

When a fuel cladding is accidentally broken and FP is discharged into the coolant, FP will have to be contained in the reactor coolant. The primary coolant pressure boundary should be reliable for that purpose.

- Barrier 4. Primary Containment Vessel

When FP is discharged as the pressure boundary is destroyed in an accident involving the rupture of piping, the containment will act as a barrier against the dispersion of radioactivity. With its excellent hermetic ability, the primary containment can significantly reduce the quantity of FP to be discharged.

- Barrier 5. Secondary containment facilities, etc.

Leaking FP from the primary containment vessel-will be retained within the reactor building and infiltrated so that radioactivity can be further diluted before reaching the neighborhood population.

## 1.2 Defense in Depth

Although there are many barriers to obstruct the dispersion of radioactive materials before they reach the surrounding environment, it is essential to ensure that these barriers effectively function without being destructed. Moreover, they should be well established in ultimate depth of their bases. A design concept called "Defense in Depth" is applied to achieve the objective, which represents a number of defense systems established in stages at the respective levels.

(1) First Level (Prevention of abnormal condition occurrences)

The primary requirement to realize the purpose of safety is to prevent the occurrence of abnormal conditions before they occur actually. The following measures are to be taken to prevent them:

(i) Each device and system shall be designed to demonstrate specified performance with ample margin, and carefully inspected and maintained to prevent any failure or damage under elaborate quality control and quality assurance systems.

(ii) The nuclear reactor core is to have negative reactivity feed back as an inherent safety feature to the operational range. It is therefore impossible for a reactor to run out of control even in case of a sudden reactivity addition, since an inherent negative reactivity will be automatically applied to suppress the increase of reaction.

(iii) The reactor shall be designed not only to maintain the integrity of the primary coolant boundary but also to confine the nuclear and thermal parameters of the core within the specified tolerable limits to prevent fuel damage despite abnormal transient changes that may occur when the reactor is operating. Therefore, no radioactivity would be discharged out of a reactor even if a failure had occurred in any of the main components or system since none of the fuel would be damaged because of the failure. Furthermore, the abnormal transient change would soon dissipate and the disorder would not be sustained for long.

(iv) The cooling boundary of the reactor is designed to have enough strength to endure postulated load, while the materials is selected so that a failure such as stress corrosion cracking can be effectively prevented.

(v) It is designed to prevent a small disorder such as a minor leak of coolant from the reactor cooling pressure boundary by detecting it in advance by a leak detection system to prevent it developing into a serious incident.

(2) Second Level (Prevention of accident Propagation)

Measures shall be taken to detect any disorder such as any kind of a failure or operational failure that may occur during reactor operation, to restore it at an early stage or to prevent it from progressing to any serious degree.

(i) Safety and protection system shall be provided in order to promptly detect occurrence of an abnormal event and automatically activate a reactor shut-down system and engineered safety failures.

The occurrence of an abnormal event can be detected by measuring various parameters that may change pursuant to the sudden rise of neutron flux levels in the reactor, a drop of the water level or pressure of the reactor or increase in the containment pressure.

(ii) The safety protection system shall be designed to have redundancy and independence, so that it will not lose function even at the occurrence of a single failure or loss of any the components or channels that comprise the system. Moreover, it should be able to eventually resume the stable condition and to perform the specified function under disadvantageous conditions such as the loss of its power source or the shutdown of the system.

(iii) The Safety protection system is designed, in principle, so that it can be tested even during operation.

As described above, the occurrence of an abnormal condition will be accurately detected and the propagation of the event will be effectively prevented.

(3) Third Level (Mitigation of the Impacts of Abnormal Event)

Various engineered safety facilities are provided in order to ensure the safety of the population in surrounding areas by preventing the propagation of the accident and reducing its impact, even in an accident which may break out despite all the above precautions. The engineered safety facilities of BWR consist of emergency reactor cooling, primary containment vessel and other related facilities. In a loss of coolant accident, which is the severest postulated accident for a nuclear plant, the engineered safety facilities will be activated to effectively mitigate the impact of the accident.

(i) Assuming a possibility that the reactor core may be exposed to air after the loss of coolant, ECCS-Emergency Core Cooling System-is designed to be initiated under such emergency situation to protect fuel rods from damages by cooling the core for an extended period.

(ii) The decay heat to be generated in the core for a long period of time shall be effectively removed out of the system with RHR-Residual Heat Removal.

(iii) Emergency power supplies shall be installed in the premises of the power station to secure the functions of the engineered safety facilities, if the outside supply is lost.

(iv) Containment shall be constructed to contain all components and systems of the reactor cooling boundary in order to confine radioactivity that may leak from the reactor and to decay over an extended period.

(v) Safety facilities such as containment spray system shall be installed to decrease the pressure by condensing steam inside the reactor containment and actively remove radioactive iodine suspending in the inside-PCV atmosphere by utilizing the scrubbing effect of the spray-system.

(vi) Flammability Gas Control System shall be installed to be operated as necessary on the assumption that flammable gas tends to accumulate in the Primary Containment Vessel (PCV).

(vii) Radioactive gas leaked from PCV shall be released into air from the main stack of ventilation system installed after radioactive iodine is removed by the filter.

## 1.3 Single Failure Criteria

The single failure criteria shall be applied to the design of systems related to the safety of the nuclear power plant.

The criteria demand a design with due considerations to the redundancy or diversity of the systems, to secure their required functions in the case of single component failure.

In case of active components such as pumps or motors, the criteria are applied to the events of both shorter and longer durations, while the events of longer duration are subject to the criteria in case of static components such as piping.

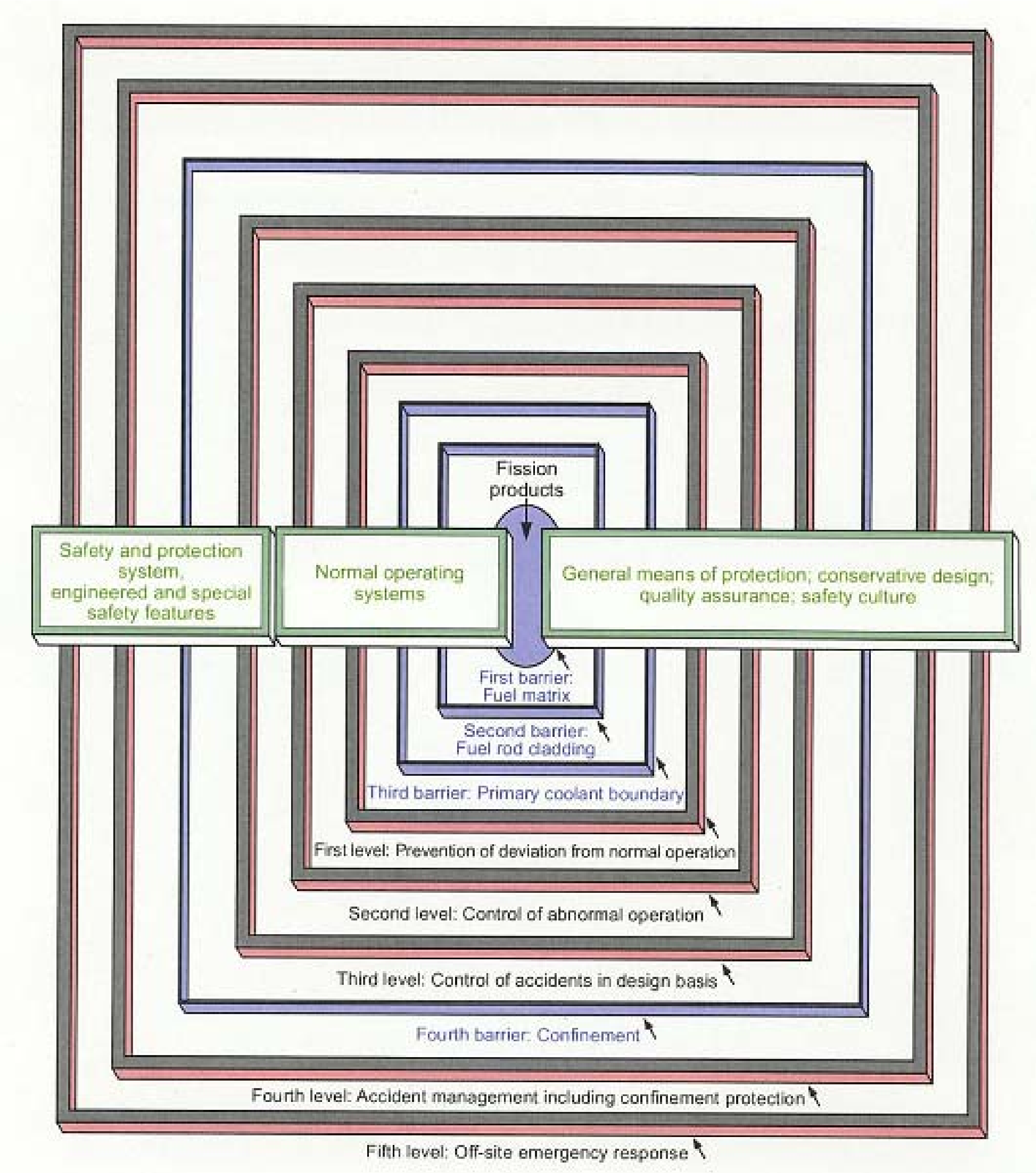



FIG.1.1 The relation between physical barriers and levels of protection in defence in depth
(From IAEA　INSAG-12)

## 2. Considerations related to the safety design of Reactor and Reaction Control Facility

### 2.1 Reactor

#### (1) Fuel

A fuel rod used for the light water reactor has a cladding made of zirconium alloy and is packed with sintered pellets of low enriched uranium dioxide. A part of the gaseous fission products generated by nuclear fission will be released from the pellet while most of the solid elements will remain in the pellet so that the pellet itself can be considered the first barrier to contain the radioactivity. Gaseous fission products released from the pellet will be sealed in the cladding. The fuel cladding is the second barrier to prevent the spread of fission products and is designed and manufactured with sufficient consideration to its quality integrity.

Fuel rod needs to be designed not to exceed the design limit of fuel during normal operation as well at the time of abnormal transient changes. It should be designed so that the maximum linear heat generation ratio will be maintained at 44kw/m or below in order to prevent the center of fuel pellet form reaching the melting point and the core will be operated with the critical power ratio of 1.20 or lower

##### (1) Reactor core

The reactor core shall be maintained critical where the generation and dissipation of neutrons is held in equilibrium, with reaction of nuclear fission corresponding to the specified output. It is controlled with the control rod possessing negative reactivity. The reaction, however, also depends on such parameters as the fuel temperature, coolant temperature and the volume of void.

The degree of changes in the level of reaction that correspond to the unit quantity of the parameter change is called the reactivity coefficient. The power output coefficient, which combines the temperature reactivity coefficient, moderator temperature coefficient and void coefficient, is designed to be negative in view of safety. This way, the self-controllability is ensured and is useful for preventing the occurrence of the abnormal conditions in the first level of "Defense in Depth" protection.

The ability to maintain the reactor in the subcriticality during operation is the ability to shut down the reactor. The reactor is designed to be able to achieve the stage of subcriticality with a sufficient margin even if one control rod of the highest reactivity had been stuck and could not be re-inserted.

The reactor will be scrammed (emergency shut-down) by the automatic activation of the reactor shut-down system if there is any risk of the reactor reaching the design limit of fuel tolerance

2.2 Reactivity Control Facility

The Reactivity Control Facility of the Reactor has a function of controlling the reactor output in order to prevent the abnormal condition, which is the first level of the Defense in Depth, and a function to shut down the reactor in order to prevent the propagation of the abnormal condition, which is the second level. It consists of the control rod, control rod drive system and the standby liquid control system, which injects bordic acid solution within 30 minutes when the control rod is not inserted.

The neutron flux in the reactor core is controlled by driving up and down the control rod containing neutron absorbing material. The control rod will be immediately inserted within a few seconds into the reactor core to shut it down at the time of emergency.

The considerations for safety are as follows:

(i) Even if a control rod was removed down out of the reactor core for some reason, dropping speed will be controlled so that a sudden application of the reactivity will be restricted.

(ii) The control rod can be quickly inserted in order to prevent a damage to occur to a fuel rod at the time of abnormal transient or accident and also to shut down the reactor by scramming at the time of an earthquake.

(iii) Measures are taken to prevent the control rod from falling down due to a rupture being caused to the control rod drive or its housing.

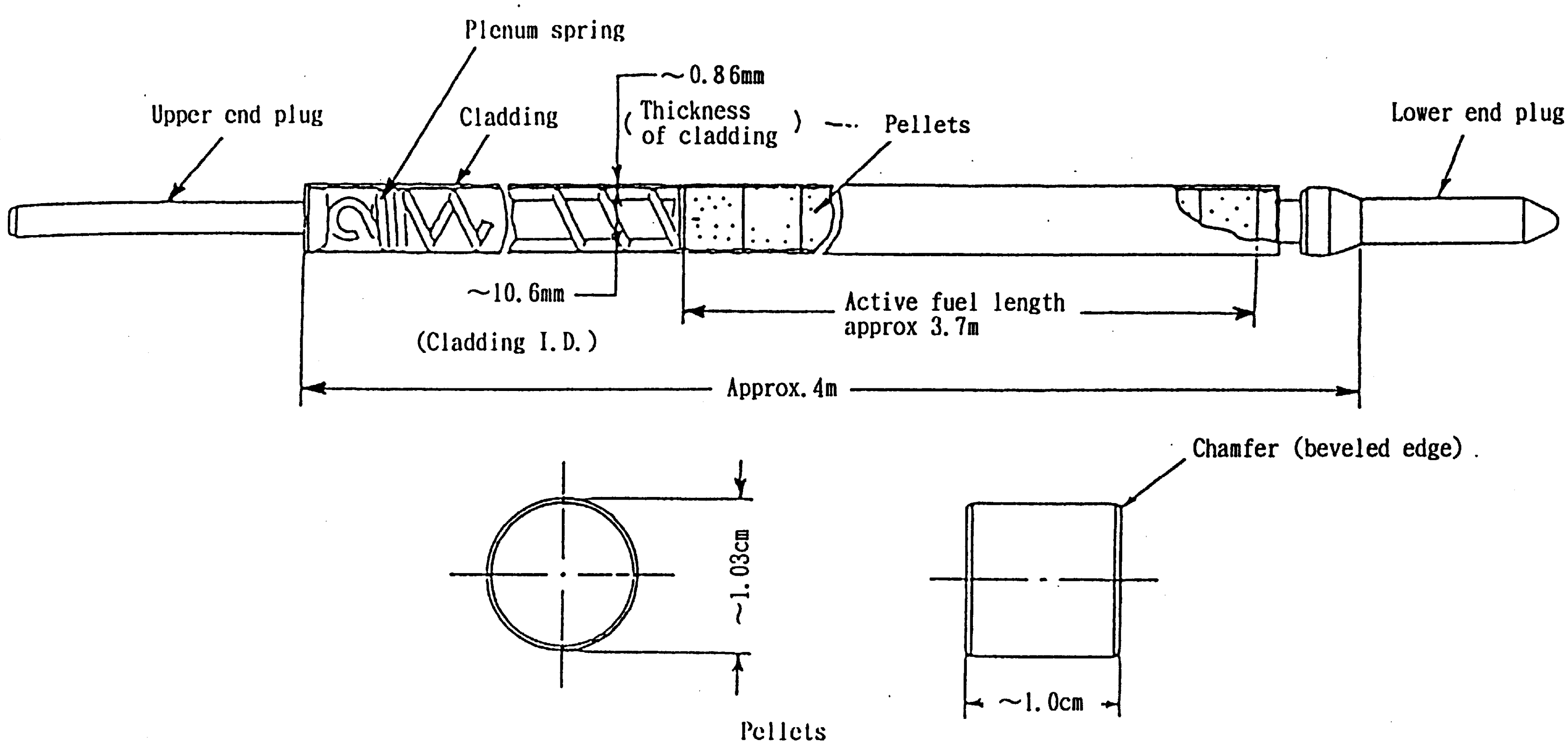



Fig.2.1 Fuel Rod

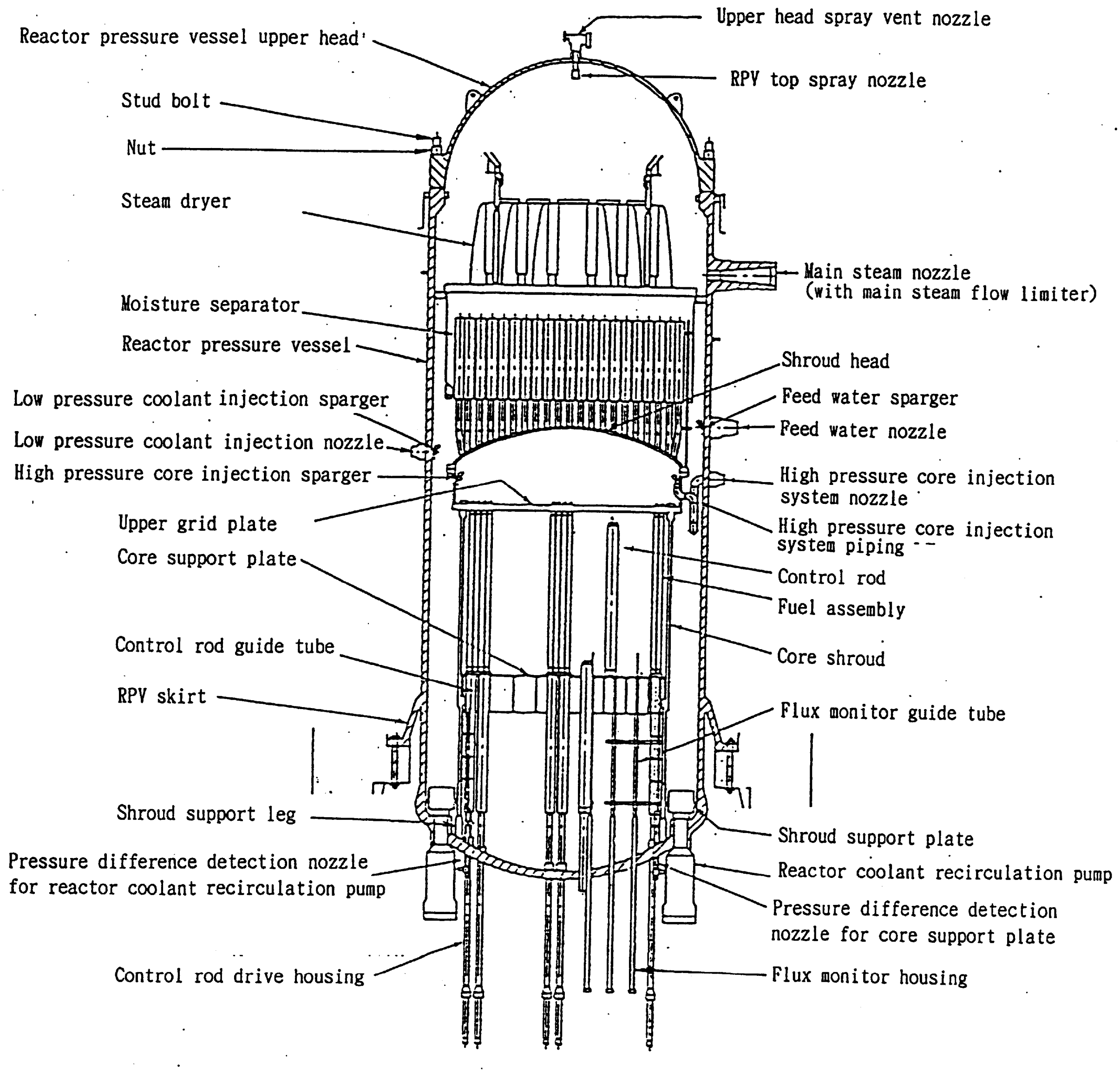
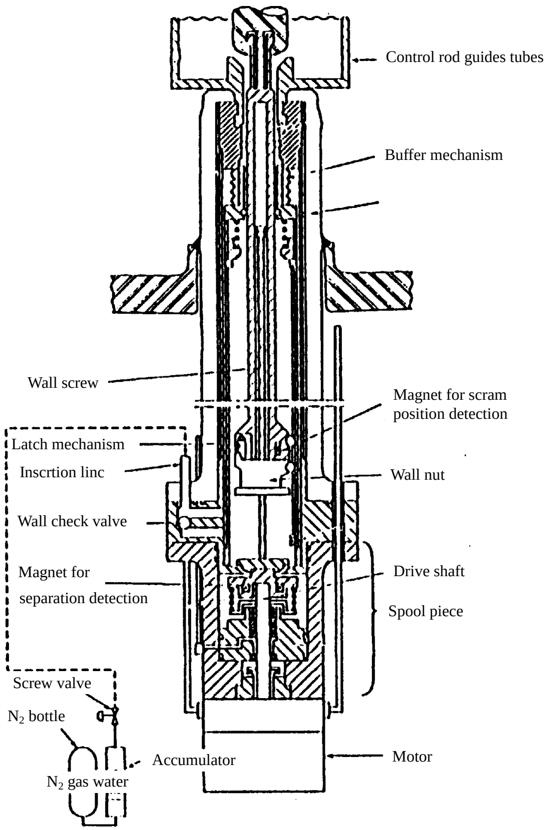



Fig.2.2 Advanced Boiling (Light) Water Reactor (ABWR)




Schematic structure of control rod drive mechanism

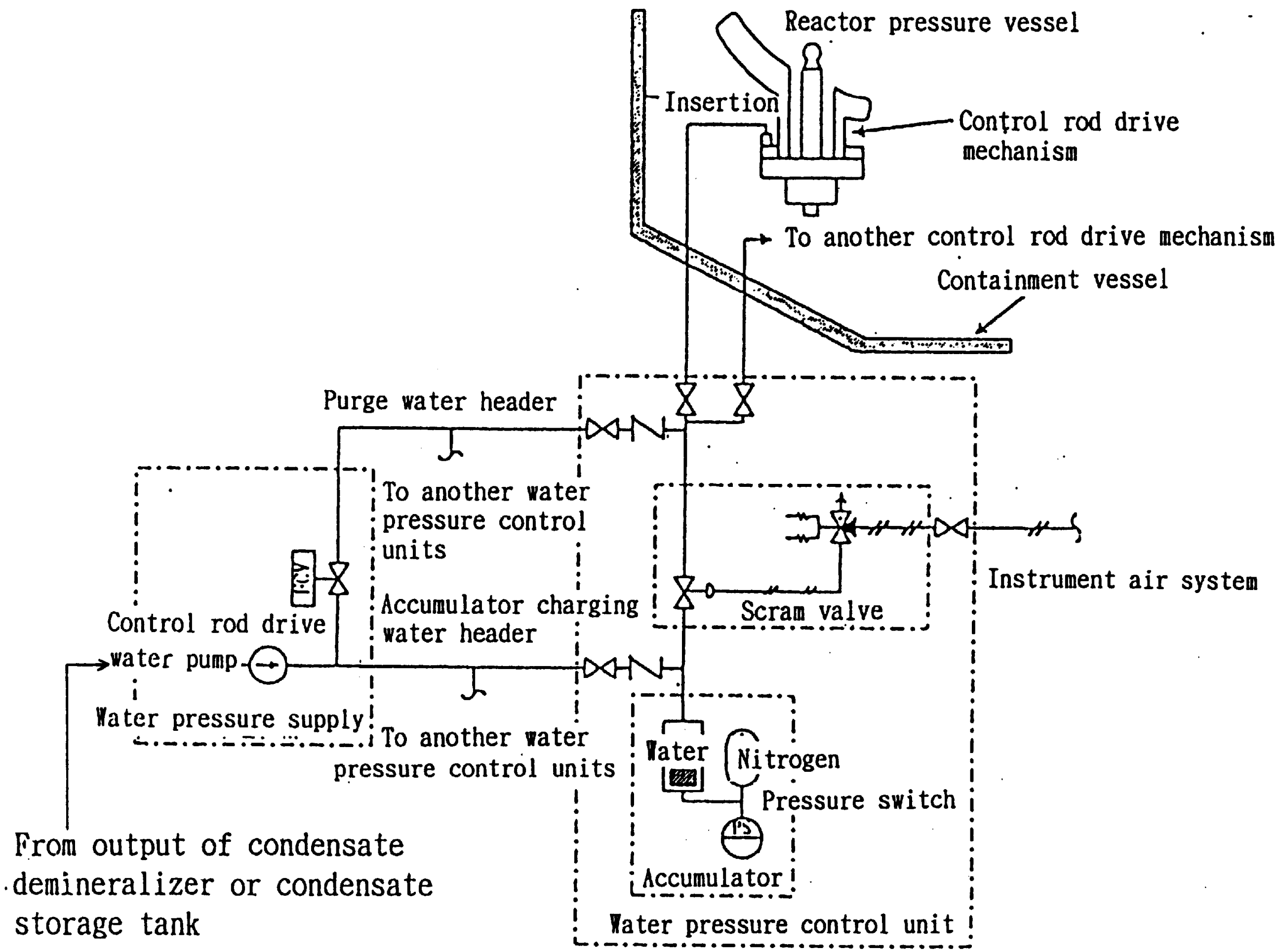



Fig.2.3 Control Drive System

## 3. Integrity of the Reactor Coolant Boundary

The reactor coolant pressure boundary is the third barrier to prevent the release of fission products (FP) provided next to the second barrier of fuel cladding. It is one of the most important factors to ensure the safety of the reactor facility because the coolant would be released if the boundary was ruptured.

The reactor coolant boundary comprises the reactor pressure vessel, a portion of the feed water system piping, a portion of main steam system piping and portions of piping and valves of other auxiliary system. Considerations are made to minimize the possibility of abnormal leakage of coolant or a loss or damage of the system by selection of proper materials, aseismatic design, and the prevention of excessive pressure, etc. Furthermore, arrangements are made to allow inspection of the reactor coolant boundary to be performed during the maintenance period while the reactor is shut down for refueling or any other reason. It is also analytically verified that the system is designed to have enough strength even in design base transient events.

For the components made of ferrite steel, due considerations are made when operating to ensure that no sudden propagating ruptures (unstable breakage) owing to brittleness would occur in the reactor coolant boundary under any operating conditions. For example, the operation of the reactor, while the temperature of the primary system is increasing or decreasing, is performed by limiting heating rate or cooling rate, and the reactor is operated by keeping itself in the safety operational range.

In a reactor pressure vessel, in particular, considerations are done in terms of material selection, design and fabrication process. The possibility of the transition temperature increase in brittleness is also taken into consideration when radiated by fast neutron. Furthermore, the minimum operating temperature, operating restrictions and other conditions are to be determined by testing with the use of the test specimen, which are fabricated from the same reactor pressure material and placed around the reactor core in capsule for a prescribed time.

It is generally recognized that a leakage can be normally detected before a crack propagates to a breakage (LBB). Monitoring and detecting systems of different measurement principles such as radioactivity monitor, the sump water system, condensation liquid measuring system are installed to monitor the leakage of the primary coolant from the reactor coolant boundary.

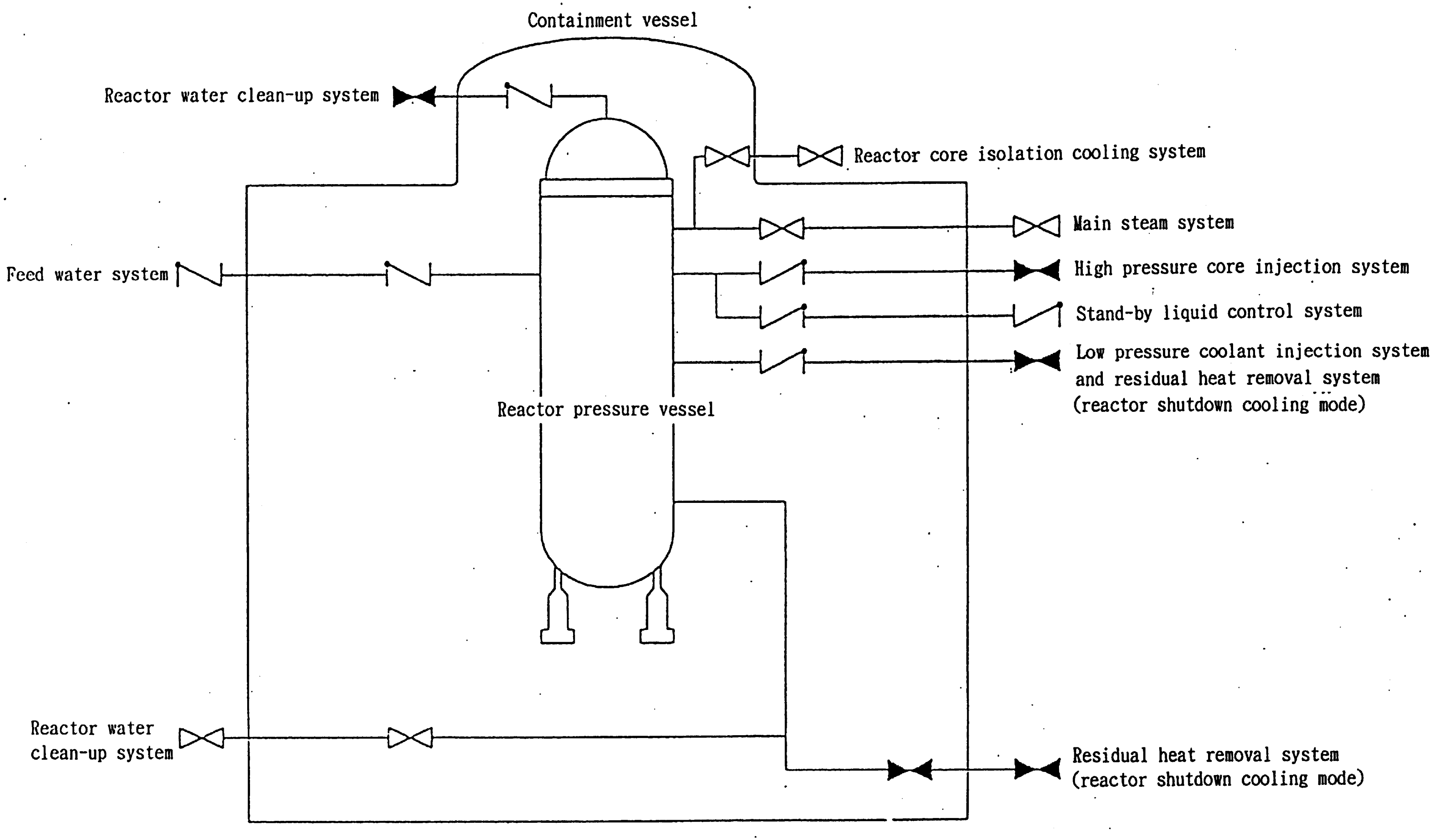



Fig.3.1 Reactor Coolant Pressure Boundary

## 4. Emergency core cooling system

The emergency core cooling system is provided to mitigate abnormal events, based on the concept 'Defense in Depth Level No. 3', and designed so as to satisfy the following requirements:

### 4.1 Design Criteria

(1) Single failure criteria and loss of external power source

In the design of ECCS, single failure criteria (Design concept 'Redundancy' should be adopted so that the system functions as specified, even if a single component fails.)is applied for active component in short and long term and for passive component in long term. Furthermore, measures should be taken against the case then the external power source is lost.

(2) Physical separation of trains

In satisfying the above single failure criteria, a component or a system is to be divided into plural small components or subsystems(trains) with the similar configuration, thus realizing redundancy. In ABWR, a design concept of 3 subsystems(trains) is adopted and the subsystems are arranged to be physically separated one another to protect the impact of damages in the other subsystem (3 division).

(3) Cooling Criteria

To prevent expended failure of fuel clad and maintain the core configuration even in case of LOCA, both fuel clad temperature and localized water-metal reactivity must be limited to the following degrees:

Max. temperature of fuel clad 1,200℃

Localized water-metal reactivity Less than 15 percent of sheath tube thickness

(4) Criteria for removal of core decay heat over a long period

The capacity for core cooling on a long term must be provided with the core configuration being maintained as it is, to remove decay heat of long half-life radioactive nuclide.

(5) There are two alternative cooling system: cooling by spray of water into the core and cooling submerging the core in water to keep down any subsequent temperature rise. The ABWR has selected the latter; the submerged cooling system.

### 4.2 System configuration

(1) Low pressure flooder (LPFL)

The LPFL is put into service when the pressure in the reactor pressure vessel is depressurized rapidly due to the accident of large diameter of rupture. It is designed to inject a large quantity of water to the outside of the reactor core shroud, by use of the low pressure injection mode of the residual heat removal system (RHR), taking water from the suppression pool.

In addition, the LPFL serves to maintain the submerged condition by water injection into the core, in combination with the other systems such as the high pressure core flooder (HPCF), reactor core isolation cooling (RCIC) and automatic depressurizing system (ADS).

The system is composed of three (3) motor-driven pumps, piping and valves. They are automatically actuated at the signals indicating 'reactor water level low (Level 1)' or 'dry well pressure high'. After recovery of the water level, large amount of water is not necessary and only making up for evaporation is required.

(2) High pressure core flooder (HOCF)

The HPCF, consisting of the motor-driven pumps, piping and valves. works functionally to cool down the core in combination with the LPFL, RCIC and ADS. The system starts its actuation at the signal of 'reactor water level low (LEVEL 1.5)' or 'dry well pressure high'. It is capable of core cooling by injection of water over the fuel assembly through the Spurger nozzle on top of the core, even if the reactor pressure remains relatively high. It has the primary and secondary water sources available for that purpose: as a primary source at first, water is taken from the condensate storage tank of primary source and if it is used up, water in the suppression chamber pool as a secondary source to perform is taken. Water feed can automatically stop at 'reactor water level high (Level 8)' after recovery of the water level.

(3) Reactor core isolation cooling system (RCIC)

In case of the ABWR, the RCIC system is designed with the function of ECCS to strengthen the high pressure system functionally. It is capable of core cooling, same as in the case of the HPCF, should any loss-of-coolant accident take place due to rupturing of the small-size piping. As one of the high pressure cooling system, it constitutes three independent systems in combination with two (2) HPCF trains.

(4) Automatic depressurizing system (ADS)

The ADS is functionally capable of core cooling, coupled with the LPFL system, when the HPCF system fails to work in case of any accident from medium or small rupturing. Upon receipt of both signals indicating 'reactor water level low (Level 1)' and 'dry well pressure high', the system can actuate, with a time lag of 30 seconds, eight (8) out of total 18 relief valves on main steam pipeline. By relief of reactor steam into the suppression chamber and rapid decrease of its pressure, it becomes possible to inject water into the core through the LPFL.

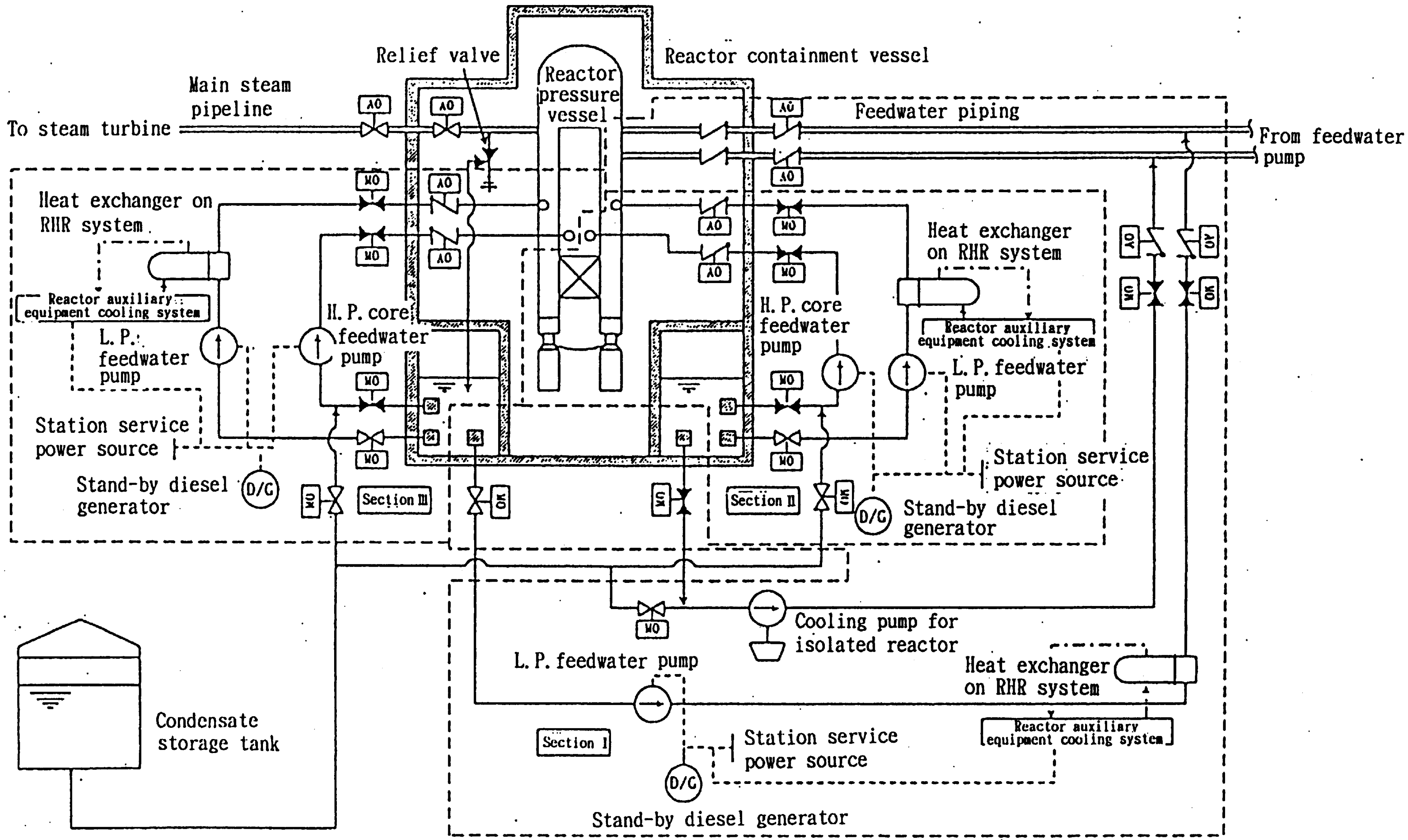



Fig.4.1 Schematic Diagram of Emergency Core Cooling System

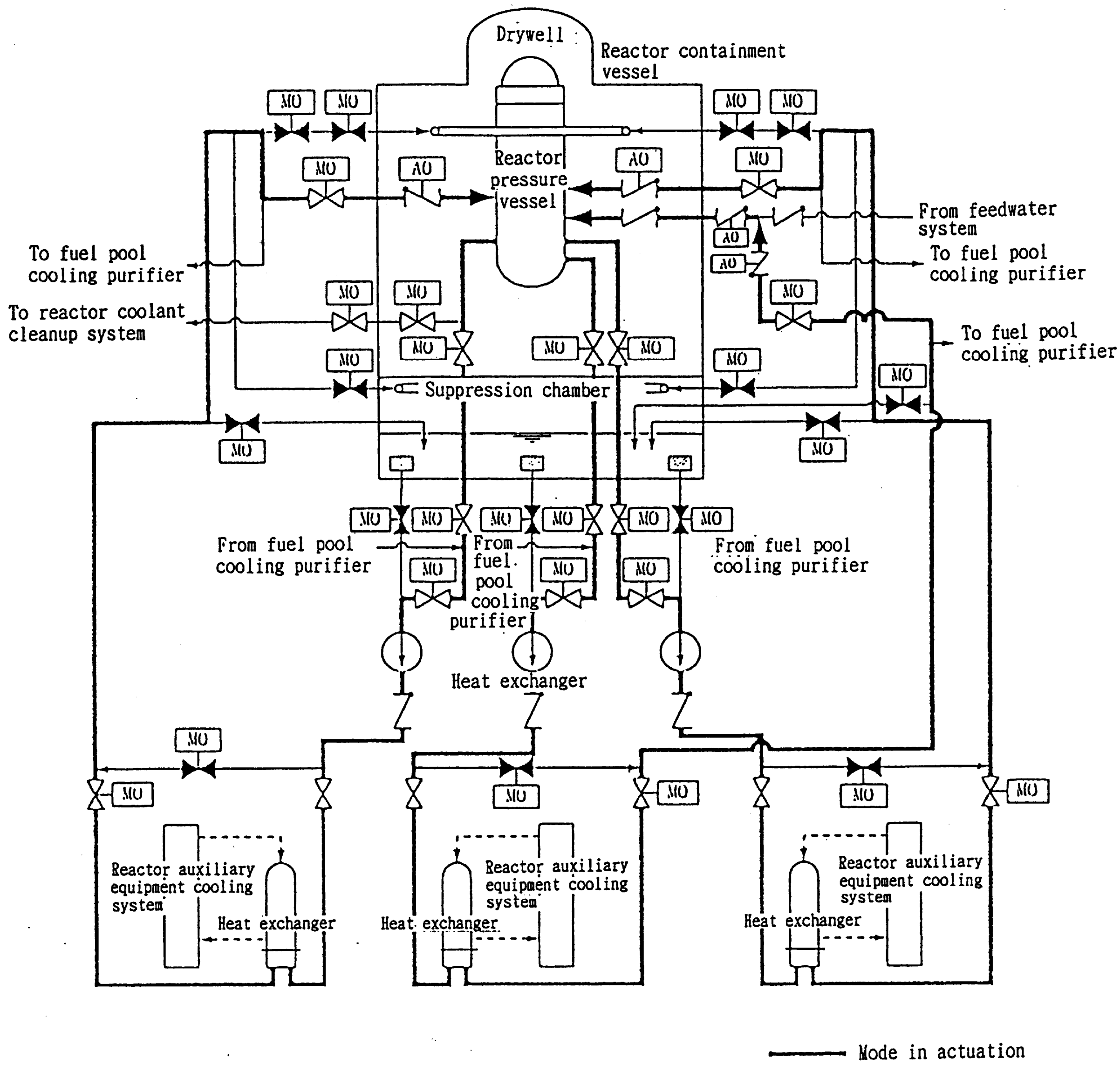



Fig.4.2 Low Pressure Coolant Injection System (LPCI)

(Schematic flow diagram of residual heat removal system at low pressure coolant injection mode operation)

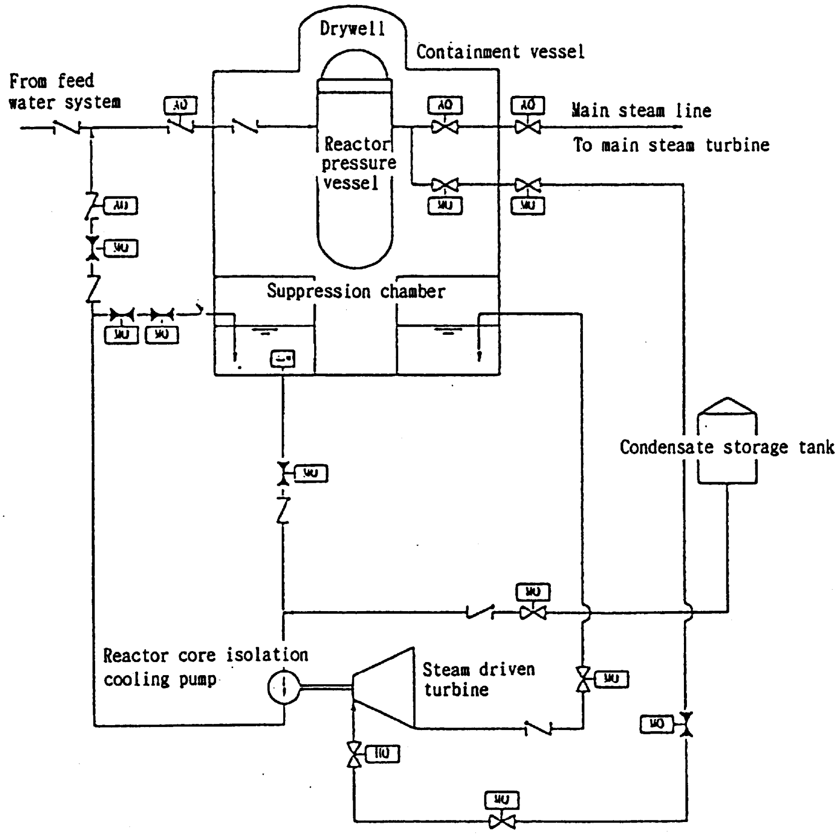



Fig.4.4 Schematic Flow Diagram of Reactor Core Isolation Cooling System

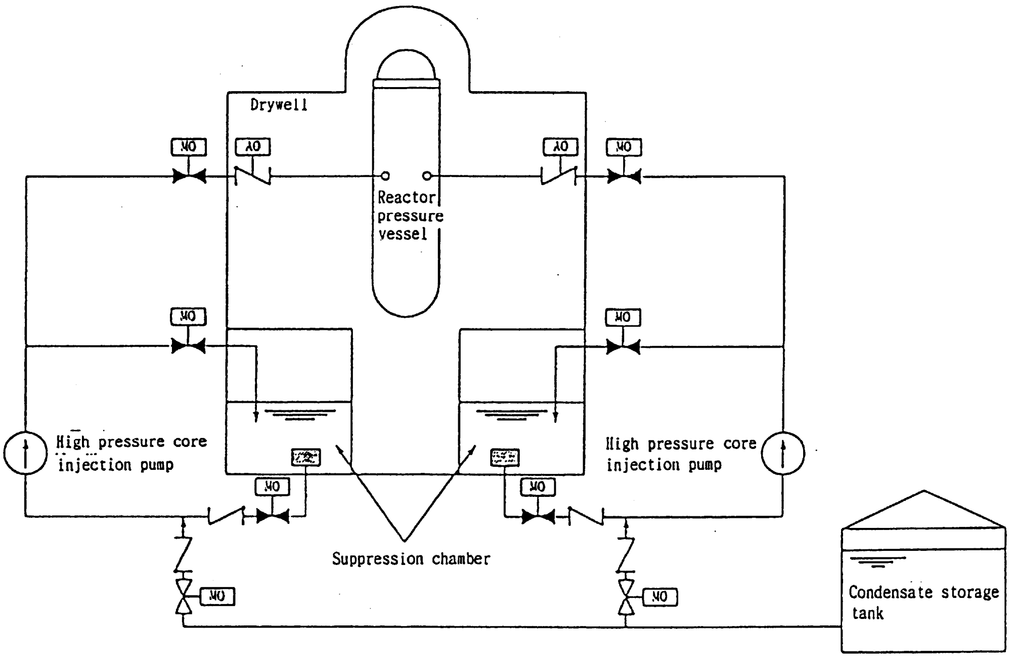



Fig.4.3 Schematic Flow Diagram of High Pressure Core Isolation System

## 5. Reactor containment facilities

### 5.1 Purpose of installing reactor containment facilities

The reactor contaonment facilities are provided, as the 4th barrier serving to confine radioactivity, for the purpose of restraining any leakage into the environment to the permissible utmost minimum level, especially for realizing the concept of defense in-depth, even if any fission products (FP) should be emitted from the core. To achieve this purpose, the reactor containment facilities consist of the primary containment vessel (PCV), the PCV spray system for cooling of internal atmosphere and removing radioactive iodine in the vessel, the combustible gas density control system to prevent combustion of gas generated from water-metal reaction in the PCV, the reactor building (secondary containment facility) to functionally prevent any leakage of fission products from direct outgoing into the environment and the stand-by gas treatment system (SGTS) designed to remove FP by filters for overhead emission through the exhaust stack.

### 5.2 Primary containment vessel (PCV)

The primary containment vessel for the ABWR is made of reinforced concrete with steel liner, inside consisting of the cylindrical dry well enclosing a reactor pressure vessel, the suppression chamber of cylindrical form and the basic slab floor. It contains the diaphragm floor of RC structure separating the dry well from the suppression chamber and the reactor pressure vessel foundation made of steel, in which the horizontal steel vent pipes are provided for connection to the dry well discharge pressure suppression chamber. The primary containment vessel has the vacuum breaker, penetration through the primary containment vessel wall and isolation valves.

In case of any loss of coolant, the mixed emission of steam and water into the dry well can be led into the pool of the suppression chamber, where steam is then cooled and condensed by water in the pool. The design requirement for PCV is to keep down any possible rise of dry well internal pressure and thereby to retain emission of radioactive materials inside the containment vessel. Therefore, the containment vessel is such designed and fabricated as to fully withstand both pressure and temperature conditions at any loss-of-coolant accident. The leak rate for the containment vessel is to be limited to 0.4 percent/d of its spatial volume at the pressure and air conditions equivalent to 0.9 time of the ordinary temperature and maximum working pressure.

### 5.3 PCV spray system

The primary containment vessel spray system constitutes two independent subsystems. Either one of them, coupled with the LPFL, can be operated to prevent any temperature and pressure rises beyond the designed limits for the containment vessel by removal of out flowing energy and decay heat of coolant resulting from rupture of the feed water pipeline, etc. It further serves effectively to clean out radioactive iodine being suspended inside the vessel. This system represents a mode of the residual heat removal system, which is designed to start up automatically as the LPFL in case of the loss-of-coolant accident and then to work functionally as the spray cooling system by remote-manual switch-over of the motor-operated valve.

The system takes water from the suppression chamber pool for spraying into the containment vessel after cooling of such water by means of the heat exchanger.

Sprayed water is returned to the suppression chamber through the vent pipes.

5.4 Flammable gas control system

The system is designed to prevent combustion of hydrogen and oxygen being generated in the containment vessel at the time of loss of coolant accident. After recombination of hydrogen and oxygen, remaining air goes back to the dry well through the vacuum breaker, so that gas concentration can be controlled in this manner throughout the containment vessel. In many cases, this system is composed of the portable recombiners of full 100 percent capacity and some others. At Unit No.6 and No.7 respectively of Kashiwazaki Kariwa Power Station, the system is arranged for common use at each reactor building.

5.5 Stand-by gas treatment system (SGTS)

The system is composed of exhaust fans, charcoal filters for iodine removal, particle filters of high performance and dehumidifiers. It can start up automatically in case of any such emergency as loss of coolant, etc. and maintain the indoor atmosphere of the reactor building at a negative pressure to check and restrain any emission of radioactivity into the environment.

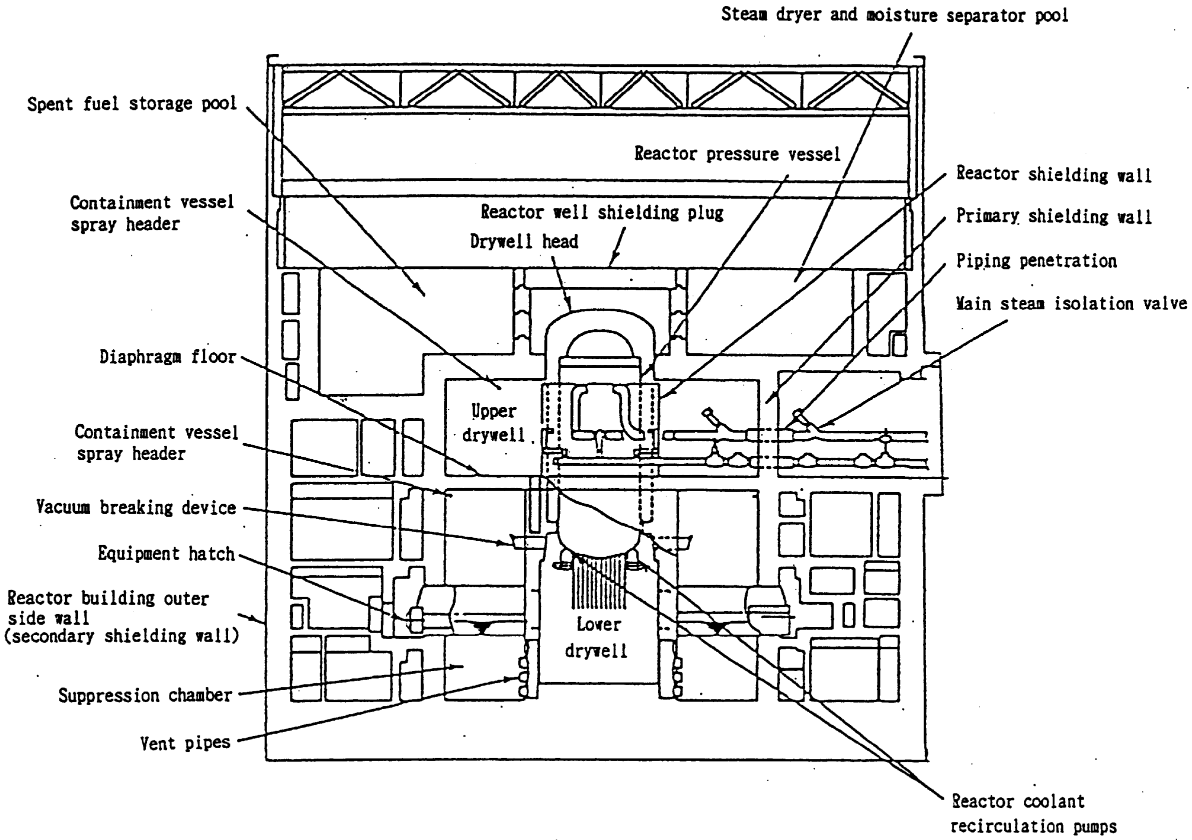



Fig.5.1 Schematic Structure of Reactor Containment Facility (ABWR)

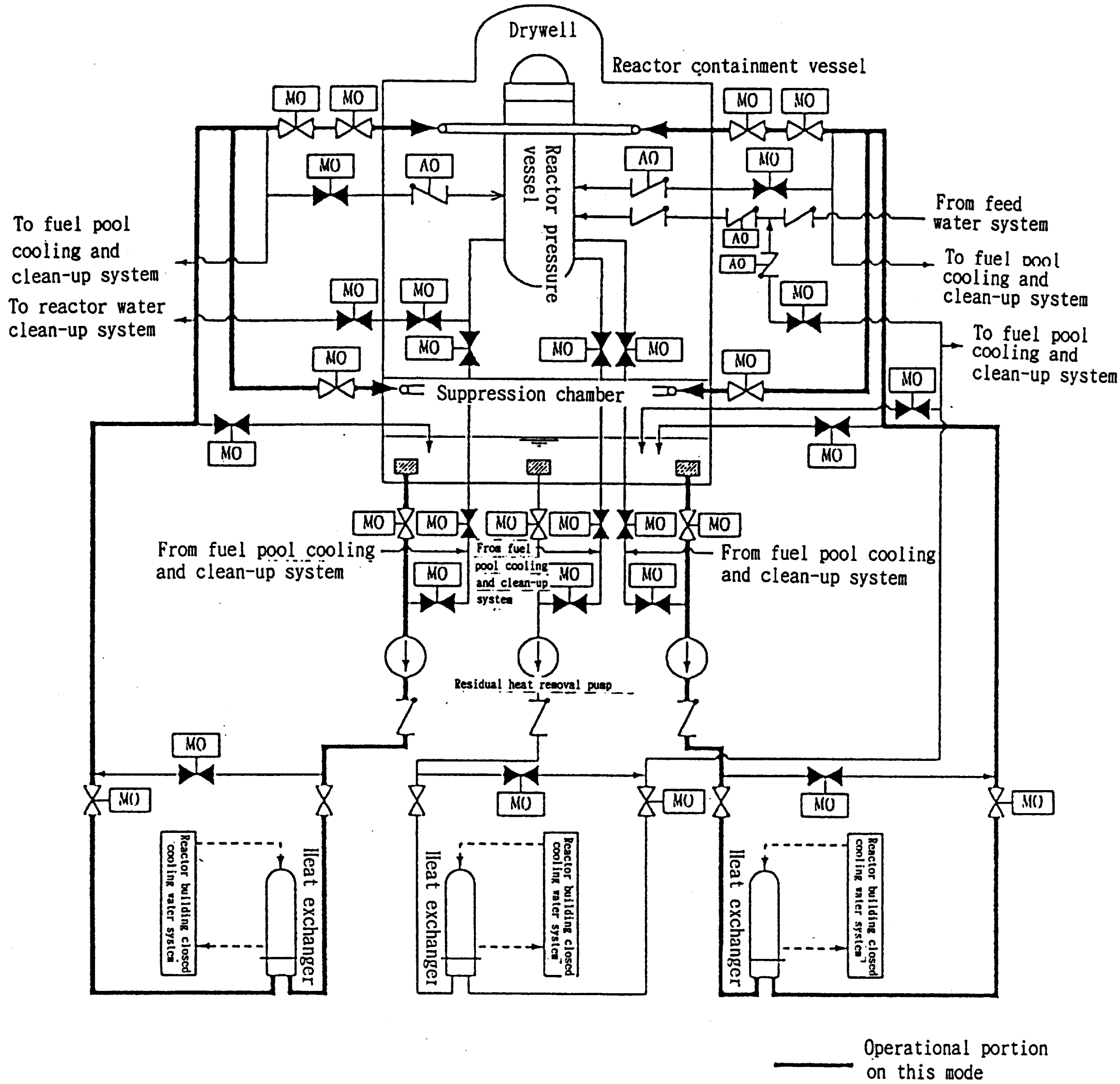



Fig.5.2 Containment Vessel Spray System (RHR system at containment vessel spray cooling mode operation)

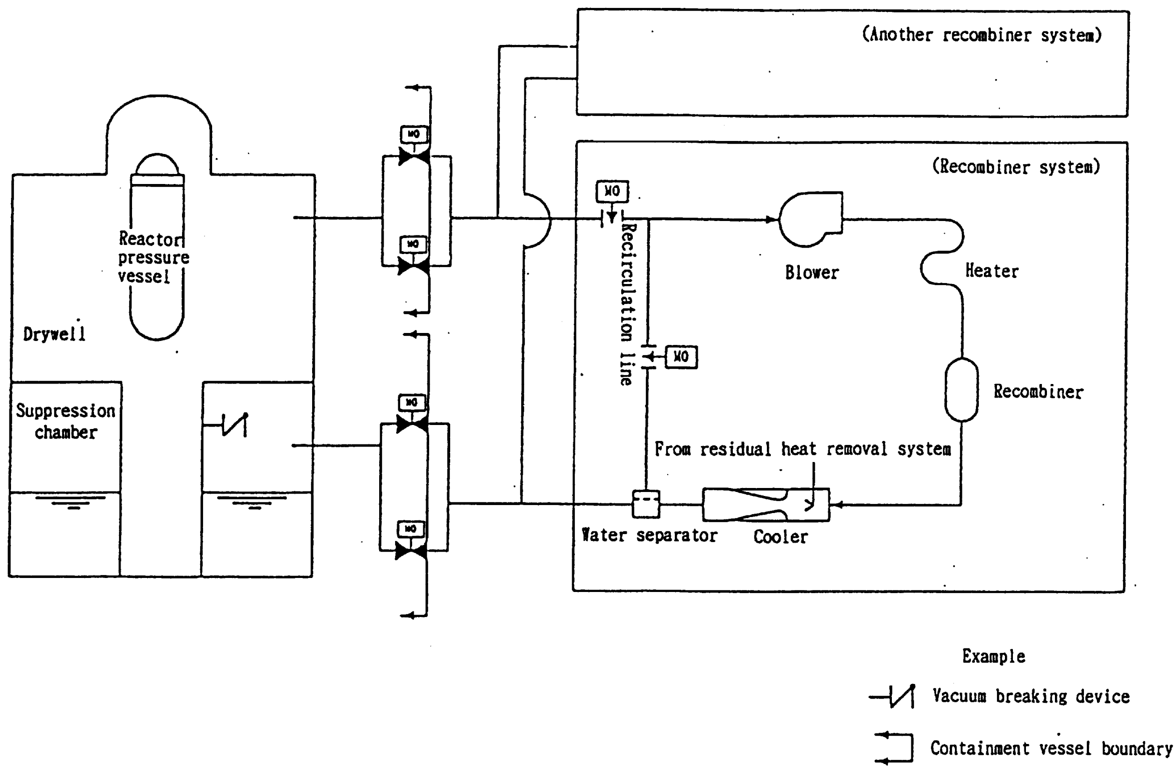



Fig.5.3 Schematic Flow Diagram of Flammability Control System

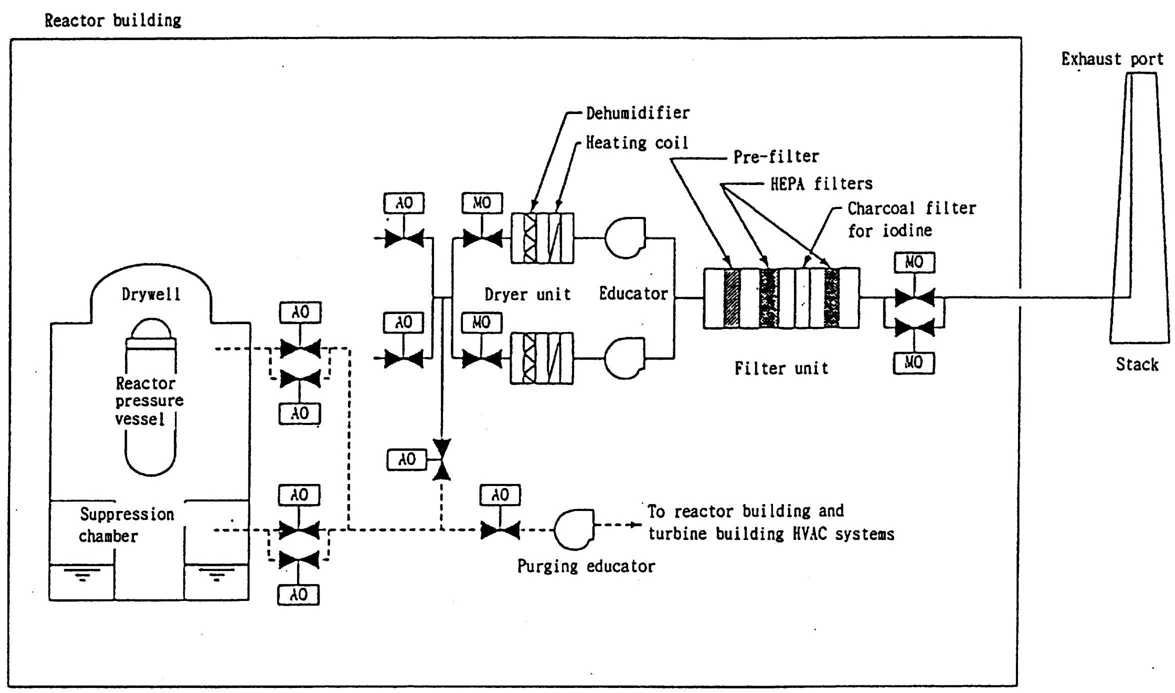



Fig.5.4 Schematic Flow Diagram of Emergency Gas Treatment System

## 6. Auxiliary systems for reactor

The auxiliary systems for removal of heat from the reactor include the following system:

### 6.1 Residual heat removal system (RHR)

The RHR system in the ABWR is composed of three (3) loop to be operated for removal of residual heats, such as core decay heat and coolant retention heat, after shutdown of the reactor. It is so designed as to meet the functional needs of multiple operating modes with one single system:

(1) Cooling mode at reactor shutdown

The cooling mode during shutdown is the most common operating mode used for removal of decay heat after shutdown of the reactor. It is so designed as to be able to cool down the reactor water temperature to 52℃ in 20 hours.

(2) Low pressure injection mode and containment vessel spray cooling mode

The residual heat removal system is used, in case of any loss-of coolant accident, as the low pressure flooder system (LPFI) for emergency core cooling and as PCV spray cooling System, while it is in the stand-by condition during normal output operation.

(3) Suppression chamber pool water cooling mode

This mode is designed functionally to take water from the pool, pressurize the water by pumps, cool down water temperature by heat exchanges and return it to the suppression chamber, whenever the water temperature of the suppression pool has risen upon delivery of steam into the suppression chamber by actuation of the main steam relief valve or the reactor isolation cooling system.

(4) Fuel pool cooling mode

This is the mode to be used for cooling the water in the fuel pool in addition to the fuel cooling system, if and when necessary. It serves as a back-up system for fuel pool cooling. if the heat temperature has gone upward beyond the capacity of the fuel pool cooling and purification system, which is provided exclusively for cooling purpose, for instance, as is in the case where the total core fuel has been transferred into the spent fuel pool.

### 6.2 Reactor core isolation cooling system (RCIC)

The RCIC system is provided for the purpose of supplying fuel cooling water into the reactor, without interruption even when the reactor has been isolated in case of the transient event. When the reactor has been isolated from the turbine facilities and the feed water system has failed to perform its function, steam will be discharged from the mainstream relief valves into the suppression chamber. If this should happen, the reactor core may be exposed after decrease of reactor water level. This is, therefor, just the time for the RCIC system to be put into operation at 'reactor water level abnormal low', thus feeding water from the condensate storage tank into the reactor. Since this RCIC system is so designed as be able to drive the turbine and the pump with use of generating steam, water feed into the reactor is still available even at the time of total power failure. In the design of ABWR, the RCIC system is operated as one of the LPFLs in the emergency core cooling system at any loss-of-coolant accident.

### 6.3 Reactor auxiliary cooling water system (RCW)

The RCW system is provided for removal of heat being generated in the components of both safety and non-safety systems and also for transfer of residual heat after emergency shutdown of the reactor into the sea as the ultimate heat sink. The system comprises three (3) subsystems corresponding respectively to each of the 3-division emergency cooling systems. Each of them can be operated for cooling independently without any loss of safety function of the total system, even on assumption of a single failure of components.

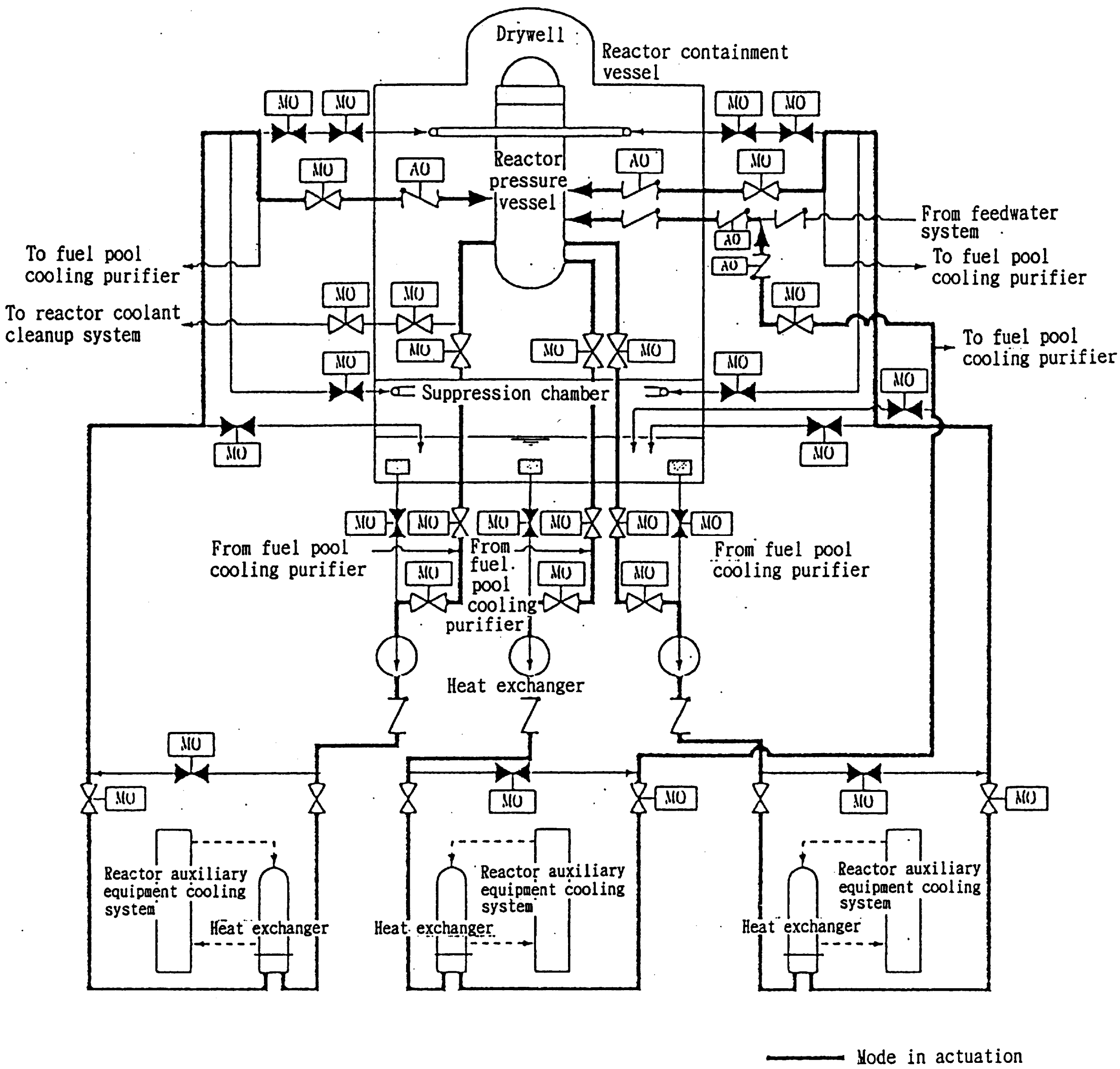



Fig.6.1 Residual Heat Removal System (Cooling Mode at Reactor Shutdown)

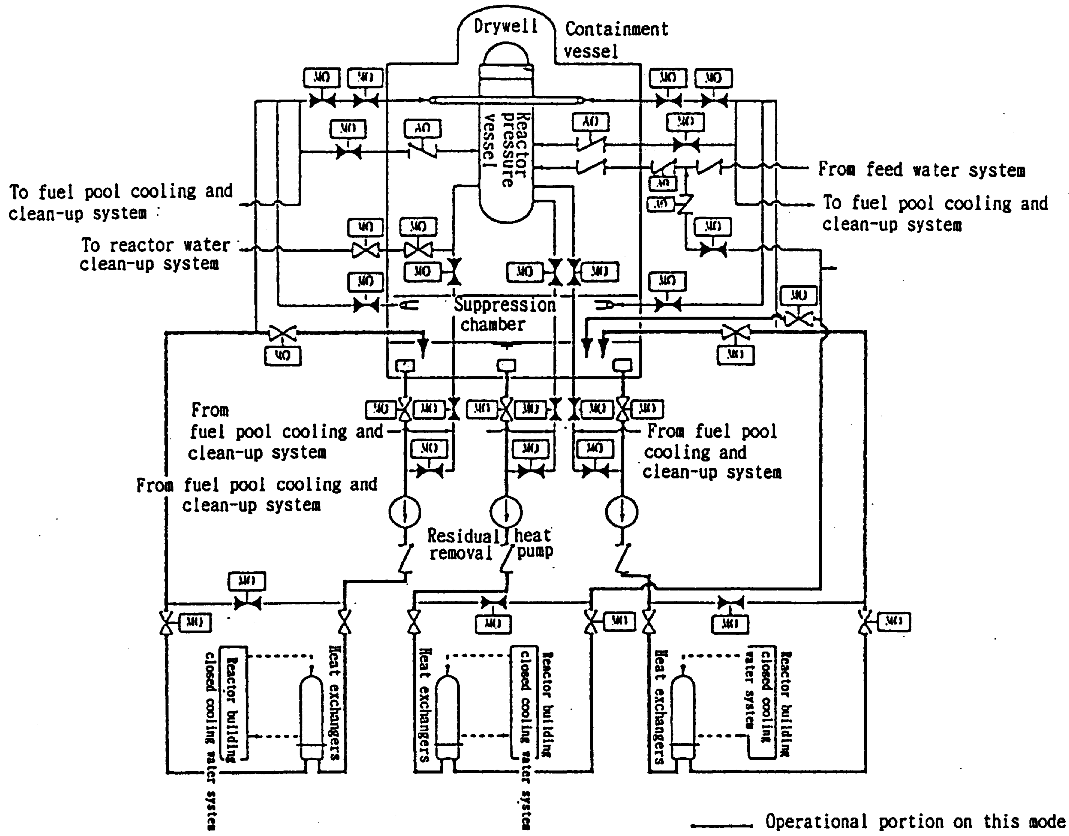



Fig.6.2 Schematic Flow Diagram of RHR System at Suppression Pool Cooling mode operation

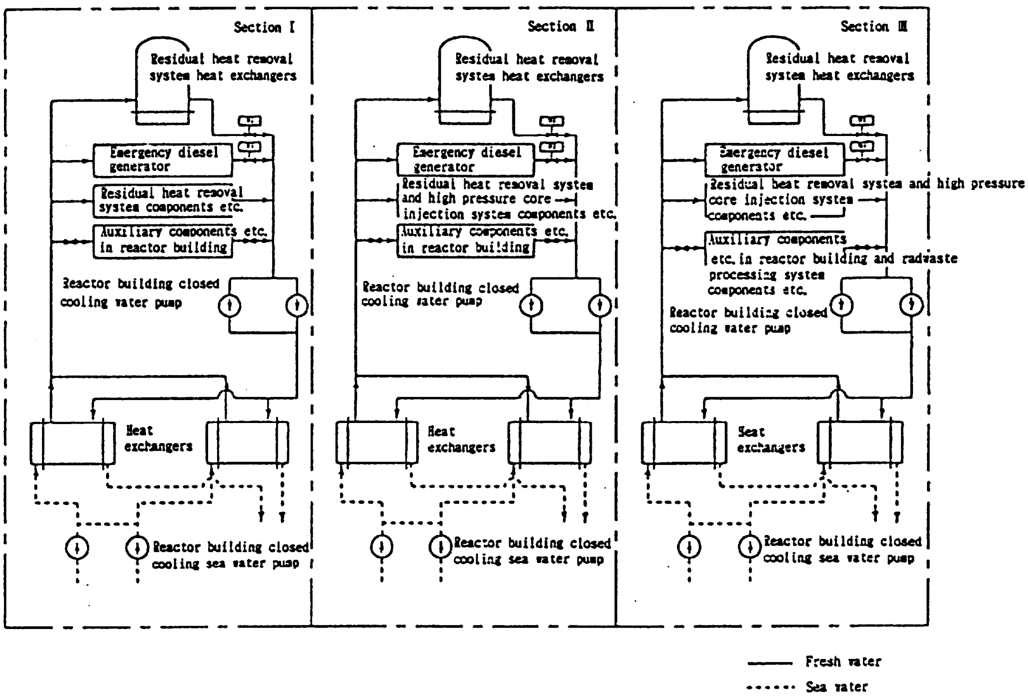



Fig.6.3 Schematic Flow Diagram of Reactor Building Closed Coolant Water System

## 7. Safety protection system

The safety protection system is provided for protection of the reactor when an abnormal transient is anticipated to occur, or, as a Defense in Depth Level No.2, to prevent further progress of the amnormal condition, which might otherwise endanger the safety of the reactor. The reactor protection system functions also, as Defense in Depth level-3, for activation of safety protection operation in order to mitigate the accident.

The protection system may generally be divided into the two categories; the one devised for emergency shutdown of the reactor in operation and the other for operation of the engineered safety system like the emergency core cooling system.

The safety protection system must be designed according to the following requirements:

a. The protection system should be designed with redundancy, being independent both physically and electrically. The primary function of safety protection should not be impaired or lost against any possible fault or failure on the single unit of equipment or when a single unit of equipment is left out of its operating condition.
b. The Protection system should be designed as to be in its permissible conditions for safety (such as 'fail safe or 'fail as is') even in the event of system power failure or loss of power source.
c. The safety protection system should be completely separated, where applicable, from the non-safety instrument control system. Even if they are partially combined together, there must be no risk of interaction between them, so that the safety protection system can be free from any failure which might take place on the non-safety instruction control system.
d. The safety protection system should be allowed to undergo periodic tests even during plant operation.
e. The safety protection system should be designed with aseismic consideration.

### 7.1 Reactor shutdown system (emergency shut down system)

In case of the earlier type reactor, (BWR-5, and earlier) all the reactor shutdown system constitute their circuits on the logic basis of (1 out of 2)× 2, while the corresponding system for the ABWR has four (4) separate system by introduction of the 2 out of 4 logic. While the conventional practice was on the basis of the analog instruments or relay sequences logic, the ABWR has its trip channel and logic circuit constituted by the digital system using the microprocessor.

## 7.2 Operating system for engineered safety system

The engineered safety system is basically activated by the reactor protection system upon detection of abnormal decrease of reactor water level or unusual increase of dry well pressure. Such events may arise from loss of coolant due to any damage on the primary system of the reactor. The low pressure core cooling system (LPFL-an operating mode of the residual heat removal system) can perform their role of water injection into the reactor core, only if and when the reactor pressure has been reduced to a lower level, because of the low discharge pressure of the pumps in operation. The automatic depressurization system can start up to reduce pressure of the reactor. when the AND-logic of 3 signals with reactor water level low, dry well pressure high and low pressure flooder in operation is satisfied.

In addition to that, the stand-by gas treatment system will be activated to maintain a negative pressure inside the reactor building, so that any possible radioactive leakage into the environment can be prevented. In order to ensure power source available for emergency, the diesel generators for ECCS must be put into service.

The operating system for engineered safety facilities in the ABWR plant is also based on the digital system by use of the microprocessor and the 2 out of 4 logic for its theoretical background is introduced.

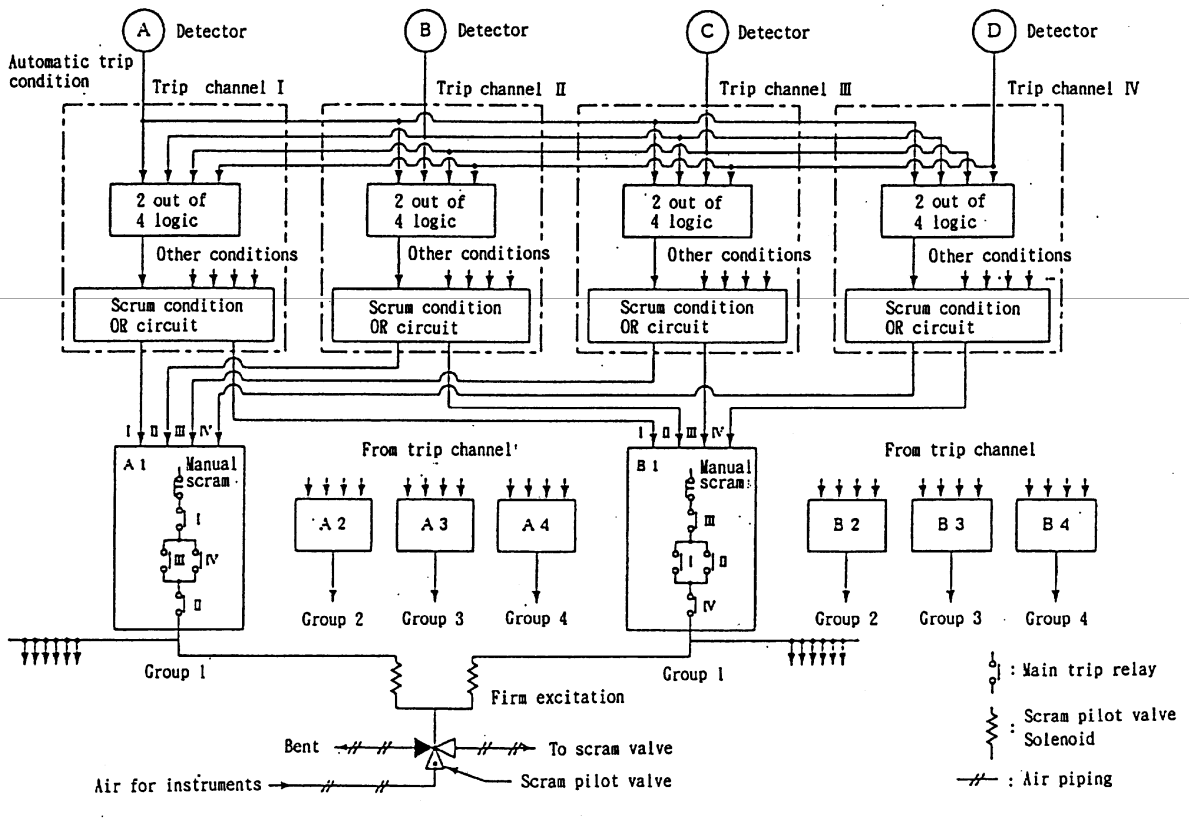
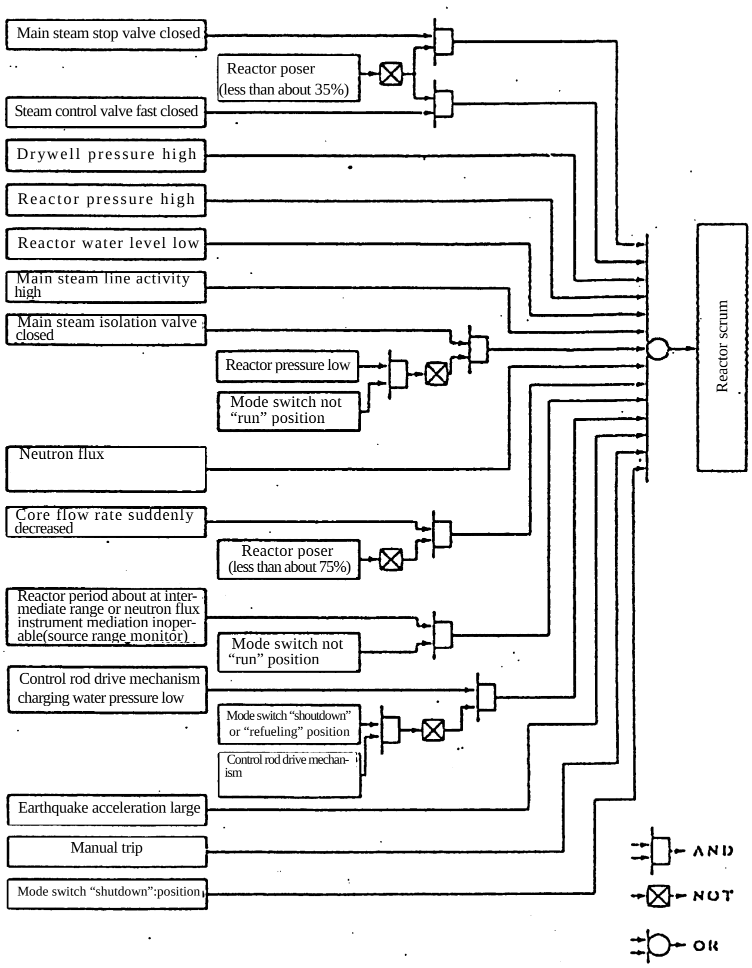



Fig.7.1 Schematic Diagram of Operating Circuit for Reactor Emergency Shutdown System

Fig.7.2 Block Diagram of Reactor Emergency Shutdown System



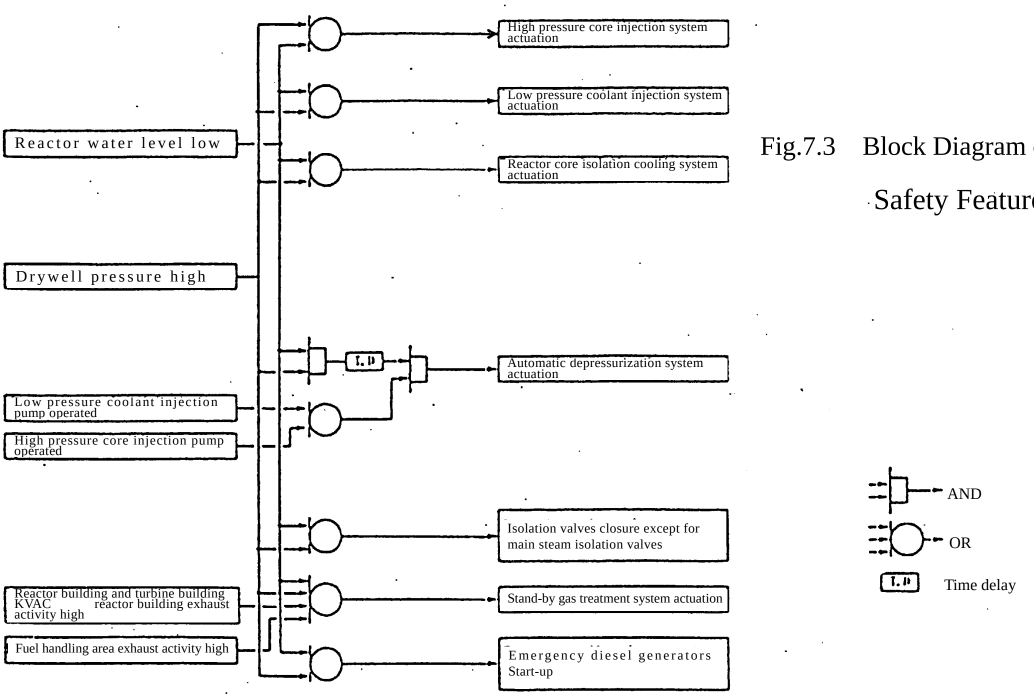




Fig.7.3 Block Diagram of Engineered Safety Feature Actuation System

## 8. Electrical system

### 8.1 Outline of design principles in safety-related electrical systems

(1) The on-site power system is provided for transmission of the generated power output to the outside service area and also for adequate power generating source to operate all the necessary auxiliary equipment of the plant for startup, normal operation and emergency operation at loss of coolant accident.

(2) The plant is provided with both off-site power supply and emergency power supply system as may required to secure the safety functions for the major buildings, structures, system and equipment.

(3) The emergency power supply system, as the power source available for all those equipment connected to the safety protection system and the engineered safety system, must be so designed as to be separated from the others electrically and physically.

(4) The design for the electrical system should ensure that, even on assumption of sigle failure, the main functions for safety protection would not be lost under the operating conditions either with the emergency power source or with the off-site power source.

### 8.2 Stand-by diesel generating set

The stand-by diesel generating set for emergency provides its service as may be necessary for the safe shutdown of the reactor when the external power system has fallen into failure. In case of the loss-of-coolant accident taking place with failure on the off-site power source, it must provides its power to actuate the engineered safety system. In view of required redundancy and independence for this system, the diesel generating system has its triple subsystem for power supply to ensure safe operation of the connected equipment on assumption of a single failure, when the external power has fallen into outage.

Diesel fuel reserved for storage in quantity is required to allow the continuous operation of the diesel generators for about seven (7) days.

### 8.3 Direct-current power supply system

The DC power supply system provides its power to the DC control circuit in the normal operational condition of the plant and in its emergency condition as well, and the supply is also at outage of the alternating-current power to the emergency power circuit.

This system, consisting of battery, electric charger and DC control center, etc., is designed with the philosophy of redundancy and each one of the redundant and isolated unit is capable of supplying electricity independently to each DC control train of the redundant safety protection systems and engineered safety systems.

8.4 Power supply system for instrument control

This system serves as the AC power supply source for control of plant instrumentation. Power is supplied by selecting an appropriate power source, depending on the required quality of power source and according to the priority of importance with regard to safety and operation of the equipment.

## 9. Characteristic features of BWR in terms of safety

In supplement to the safety design of BWR as outlined above, the characteristic features of BWR in terms of safety may be summarized in the following:

(1) Self-controllability of power output

The first one of the features is that there is generation of void (steam foaming) due to boiling of coolant at the core during normal operation. This implies that when the output increases for some causes, the degree of boiling water tends to increase accordingly with resultant reaction toward reducing the thermal neutron flux, thus effectively suppressing the rate of power output increases.

(2) Large cooling capability by natural circulation

The second feature is that the BWR has a large capacity of natural circulation which is, in itself, capable of removing core heat at and up to about 50 percent output, even though the recirculation pump has suspended its operation.

(3) Monitoring of water level

The third point of its features lies in the full-time direct monitoring over the reactor water level by means of the level gage. The control system is such designed that the water level can be automatically adjusted by regulation of the feed water flow if and when the level gage indication is varied.

(4) Water pooling in large quantity

The fourth point refers to plenty of water reserve in the pool inside the suppression chamber of the primary containment vessel. Because of this reserve, decay heat to be generated in the core can be absorbed for some time into the pool: even if the circumstance demand complete separation of the reactor. Furthermore, even on assumption of the loss of coolant accident (LOCA) caused by damage on the primary coolant system, the reservoir pool serves to absorb thermal emission and is functionally capable of feeding water into the emergency core cooling system (ECCS) over a long period, thus contributing much toward higher safety.

# APPENDIX TO OUTLINE OF SAFETY DESIGN

# (CASE OF BWR)

OUTLINE OF SAFETY DESIGN
IN
ABWR

1. Purpose of ABWR Development

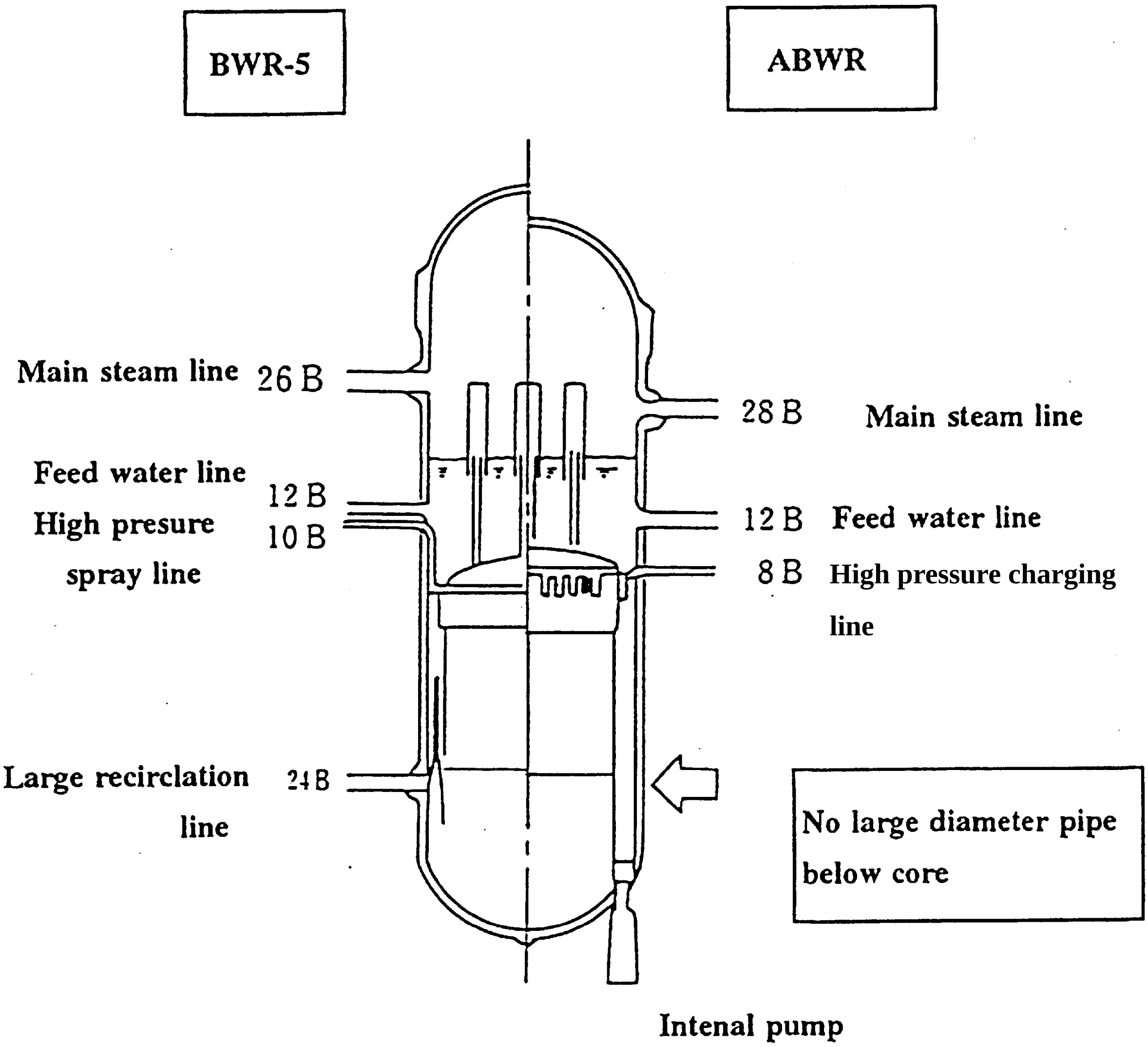
   - Improvement of Safety and Reliability
   - Improvement of Operability and Maneuverability
   - Reduction of Radiation Exposure

2. Reduction of Postulated Pipe Rupture Diameter
   (Internal Pump)
   Elimination of Large Recalculation Piping

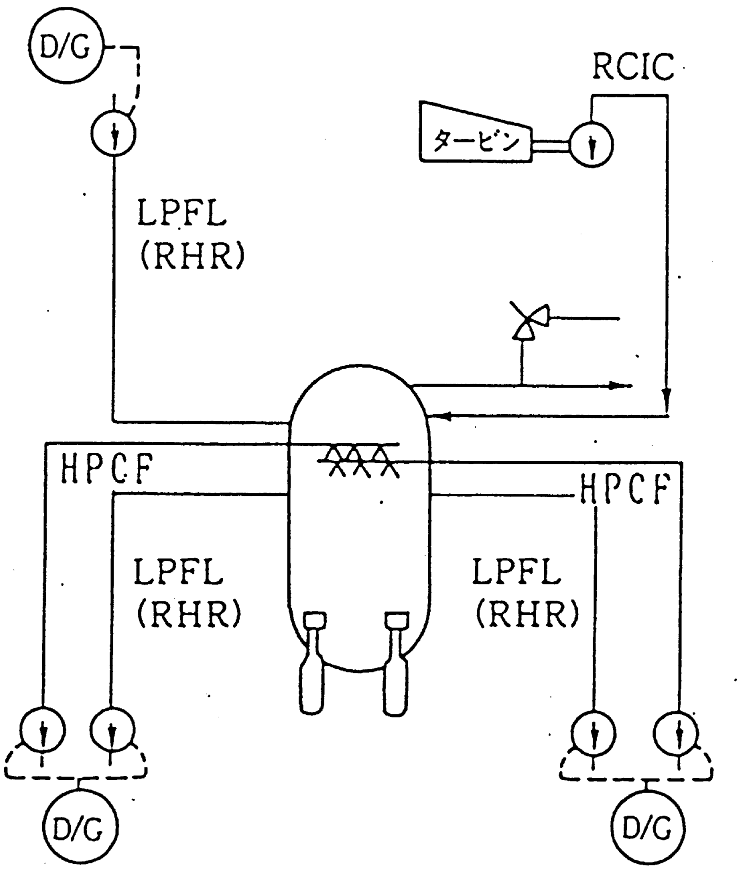
3. Improvement of Reactor Shutdown Capability
   (Fine Motion Control Rod Drive Mechanism)
   Diversity of Driving Source
   Hydrauric Scramming
   Electrical Motor Drive Insertion
   Normal Drive
   Fine Motion by Electrical Motor

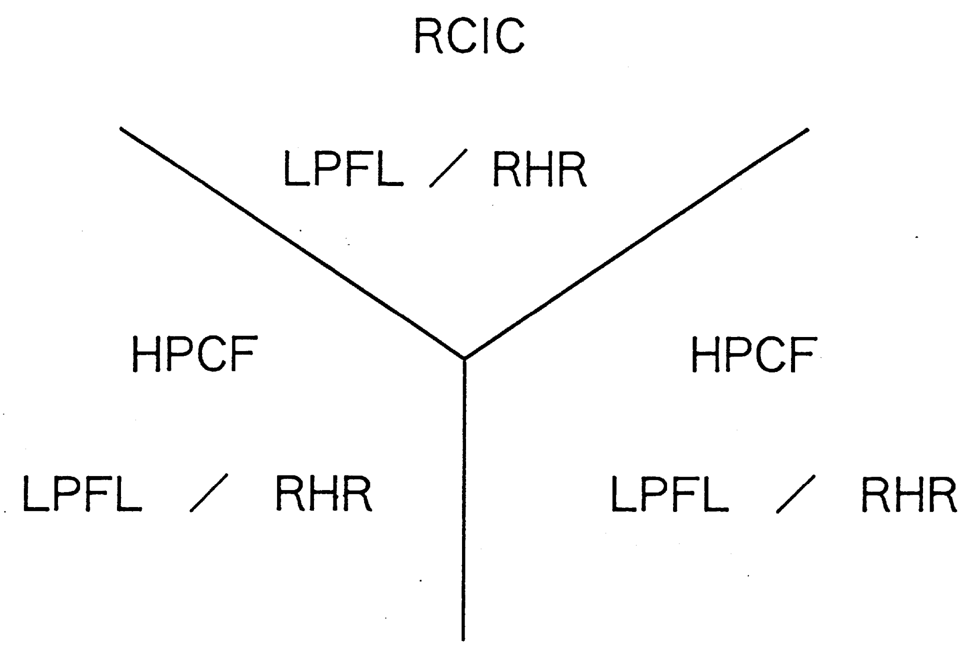
4. ABWR Technical Features and Plant Performance

| PERF. / Tech. Feature | Plant Safety | Plant Availability | Plant Operability | Radiation Exposure Reduction | Economic Rationaliza-tion |
|---|---|---|---|---|---|
| 1. Large Capacity | | | | | ○ |
| 2. Improved Core | | ○ | ○ | | ○ |
| 3. Internal Pump | ○ | | ○ | ○ | |
| 4. Fine Motion CRD | ○ | ○ | ○ | ○ | |
| 5. Three-division ECCS | ○ | | | | |
| 6. RCCV | ○ (Aseismatica-ly) | | | | |
| 7. New I&C | ○ | ○ | ○ | | |

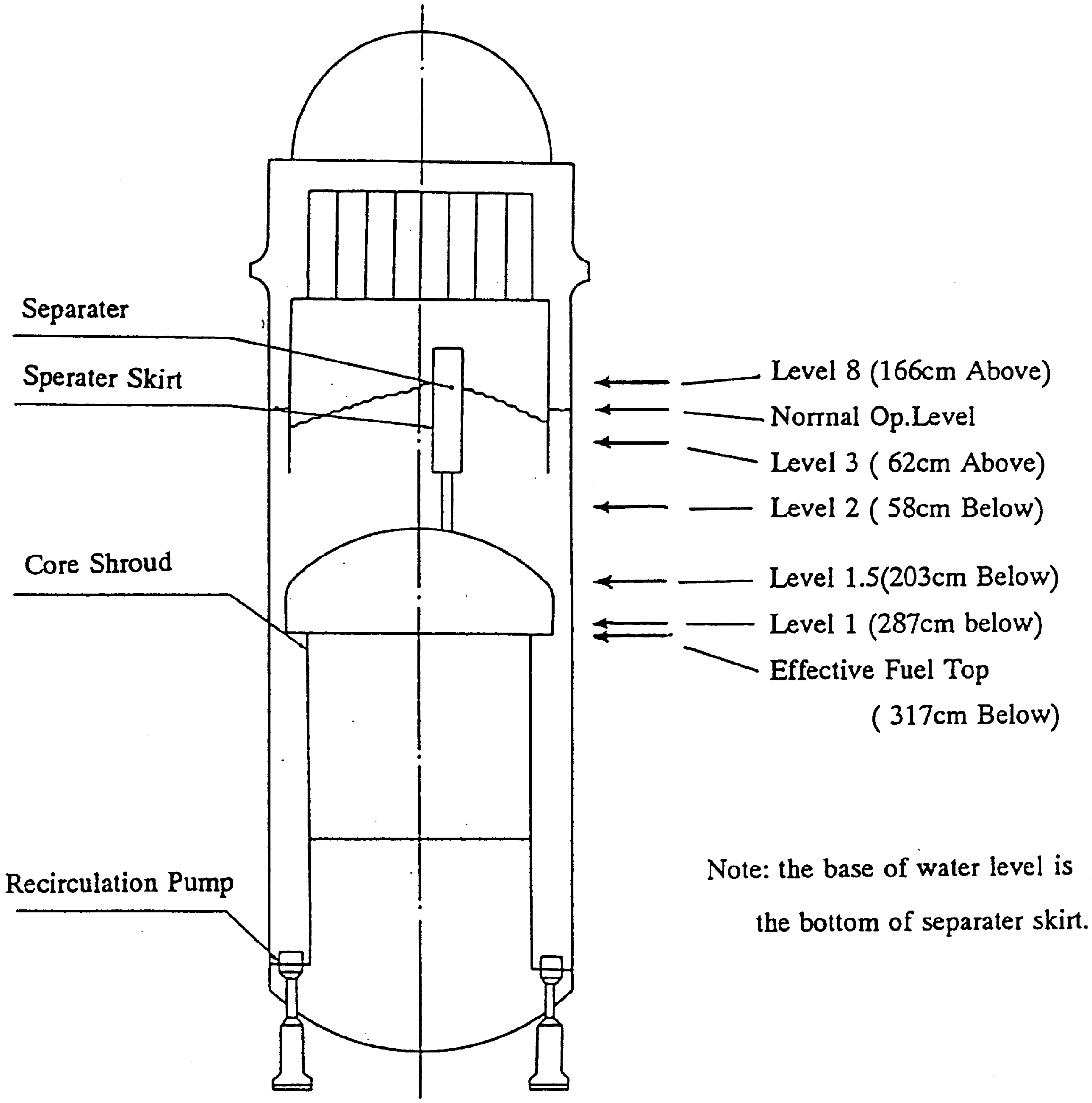



Elimination of Large Recirclation Pipe By Adaptation of Internal Pump




3-Division In ABWR ECCS




Water Level In Reactor Core

Function of Water Level Signal

| | |
|---|---|
| Level 8: | Turbine Trip |
| | feed Water Pump Trip |
| Level 3: | Reactor Scram |
| | 4 Recirculation Pumps Trip |
| | Stand-by Gas Treating System Start |
| Level 2: | RCIC Start |
| Level 1.5: | HPCI Start |
| | MSIV Closure |
| | D/G (Div. II III)Start |
| Level 1: | LPFL Start |
| | Ads Start |
| | D/G (Div. I)Start |

(OHP PRESENTATION MATERIAL)

# OUTLINE OF SAFETY DESIGN

# (CASE OF BWR)

# Outline of Safety Design
## (Case of BWR)

September, 2005

Japan Nuclear Energy Safety Organization

# Concept of Safety Design in Nuclear Reactors

- 3 Principle of Reactor Safety

  1. Shutdown

     Reactor shutdown at abnormal condition

  2. Cooling

     Residual heat removal

  3. Contain

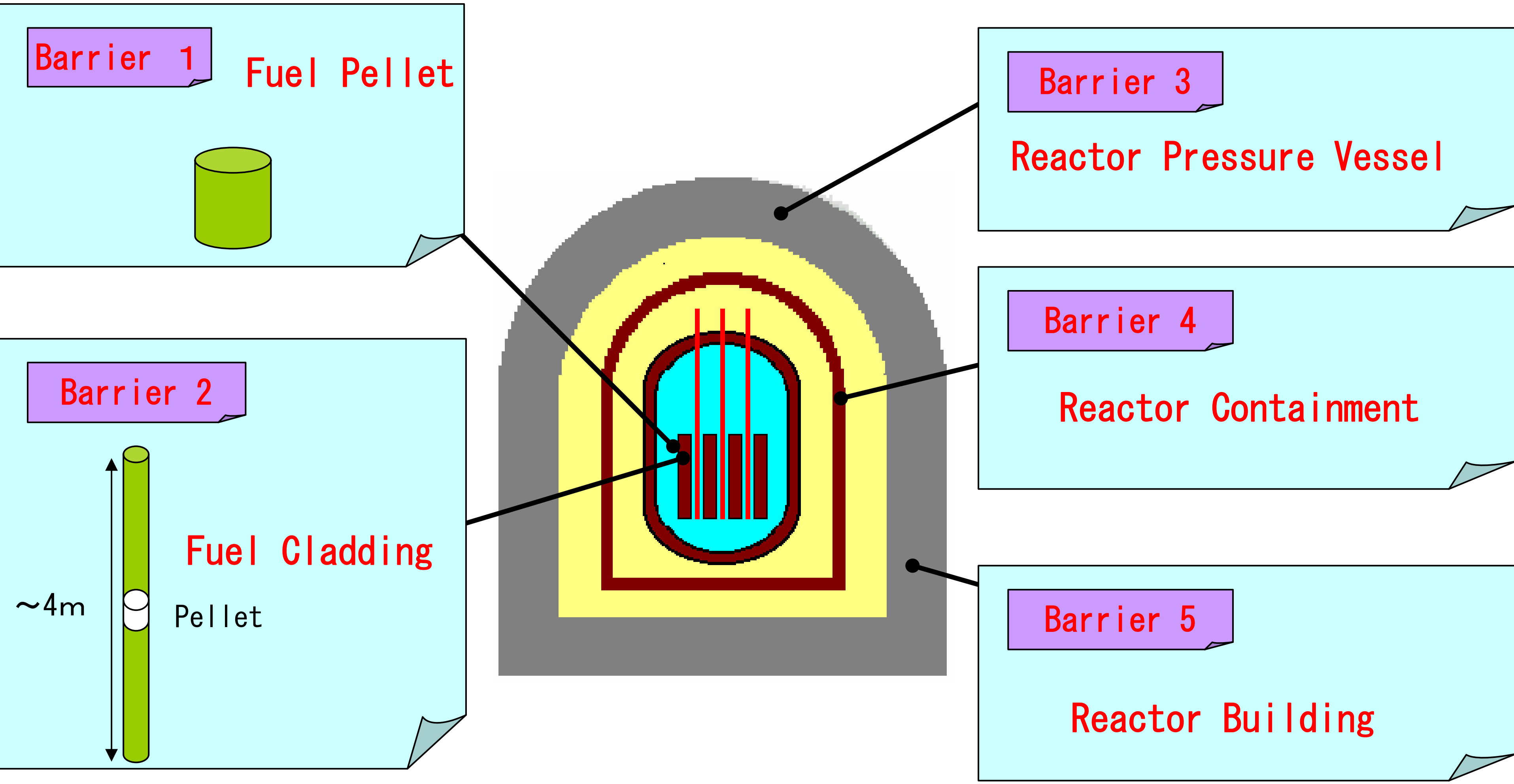
     Contain of radioactivity

# Multiple Physical Barriers

- 5 Barriers for Containing Radioactivity
  - Level-1: Fuel Pellet Matrix
  - Level-2: Fuel Rod Cladding
  - Level-3: Reactor Primary Coolant Pressure Boundary
  - Level-4: Primary Containment Vessel
  - Level-5: Secondary Containment Facilities

# Protective Barrier for Containing Radioactivity

## -Quintuple Barriers-



# Defense In Depth

- 3 levels defense

☆First level (Prevention of Abnormal Conditions)

● Design Margin

● Careful Maintenance

● Quality Assurance

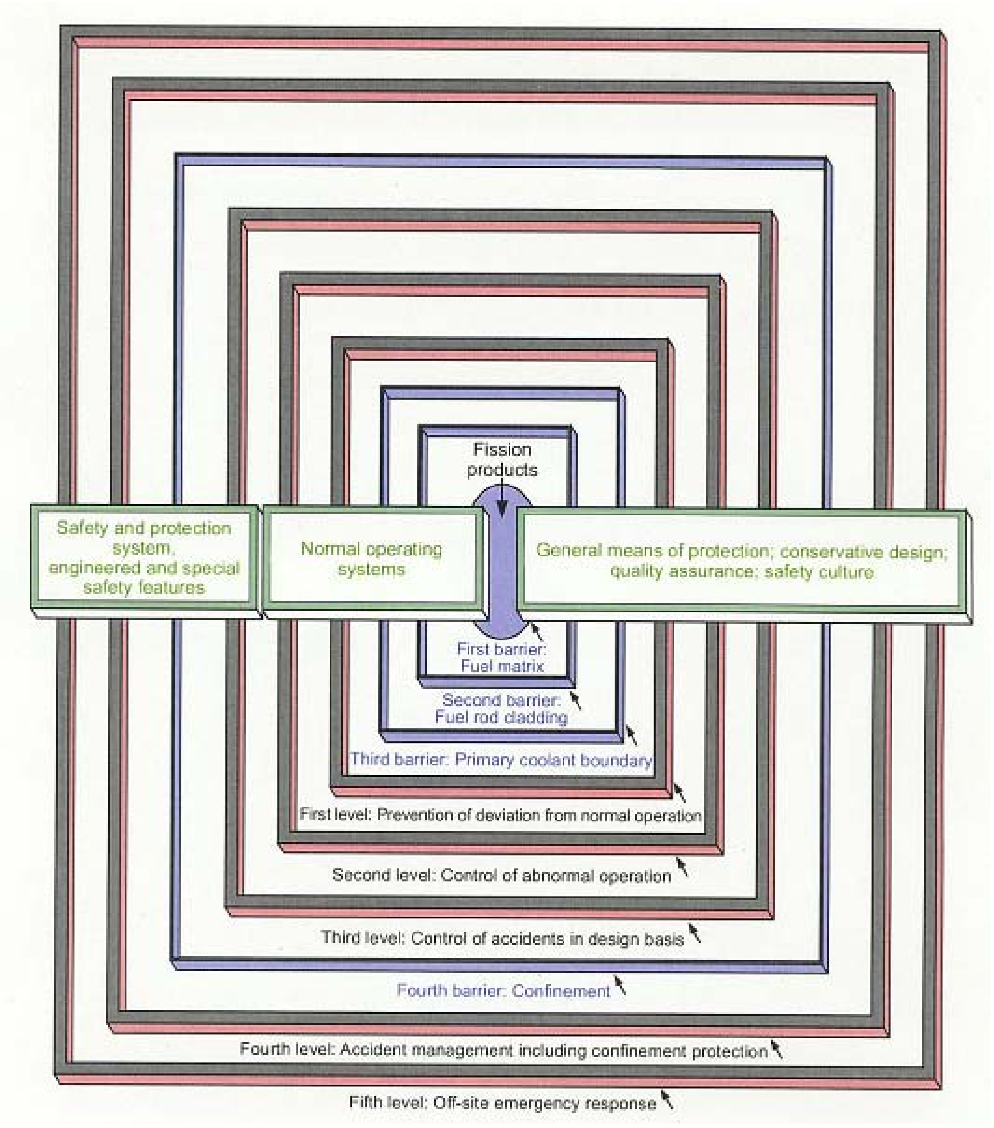
☆Second Level (Prevention of Abnormal Condition propagation)

● Detection of Abnormal Condition (Reactor Shutdown)

☆Third Level (Mitigation of Abnormal Condition)

● Emergency Core Cooling System

● Confinement of Radioactivity in Containment




The relation between physical and levels of protection in defense in depth

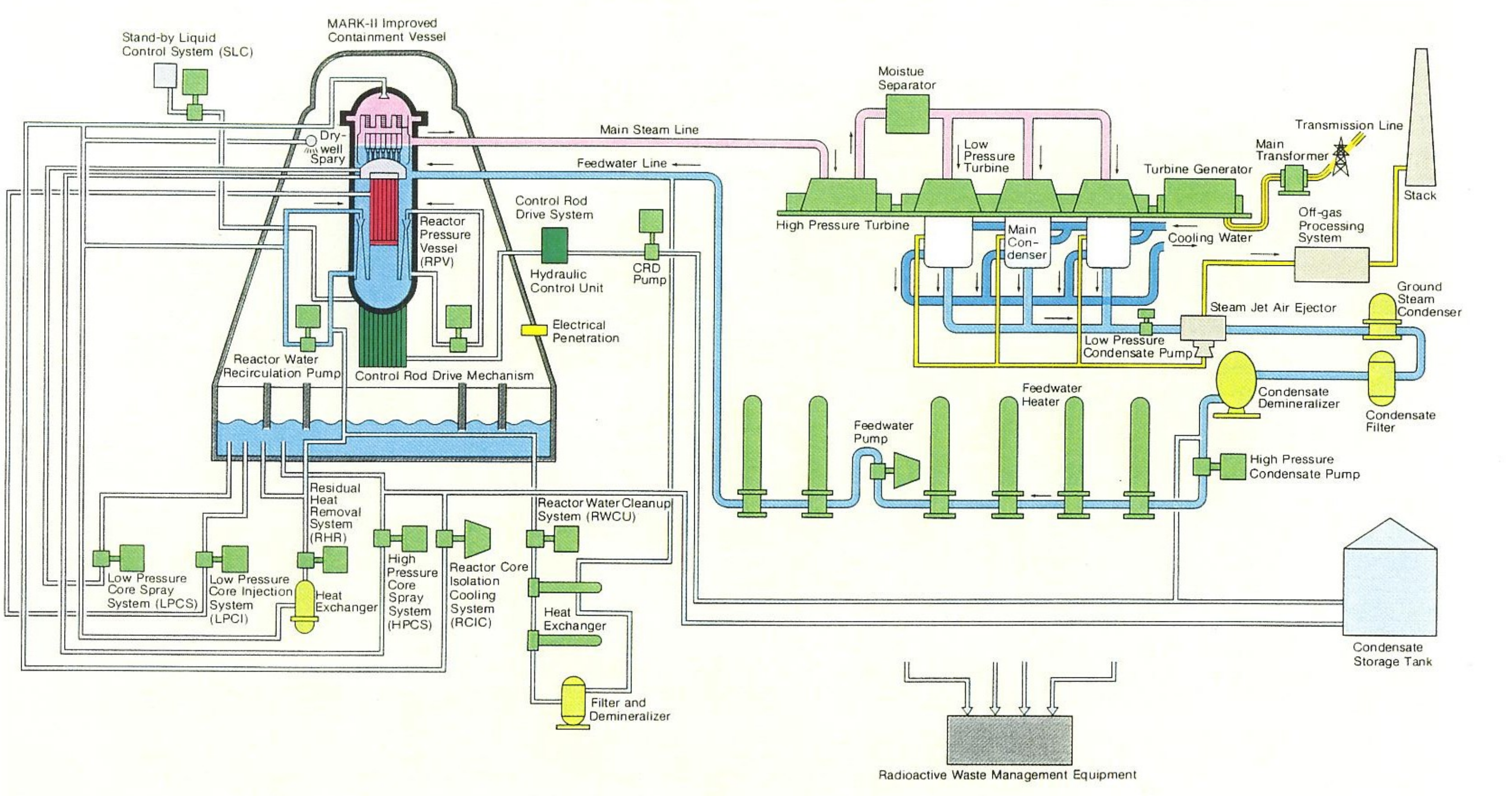
# Single Failure Criteria

- Definition

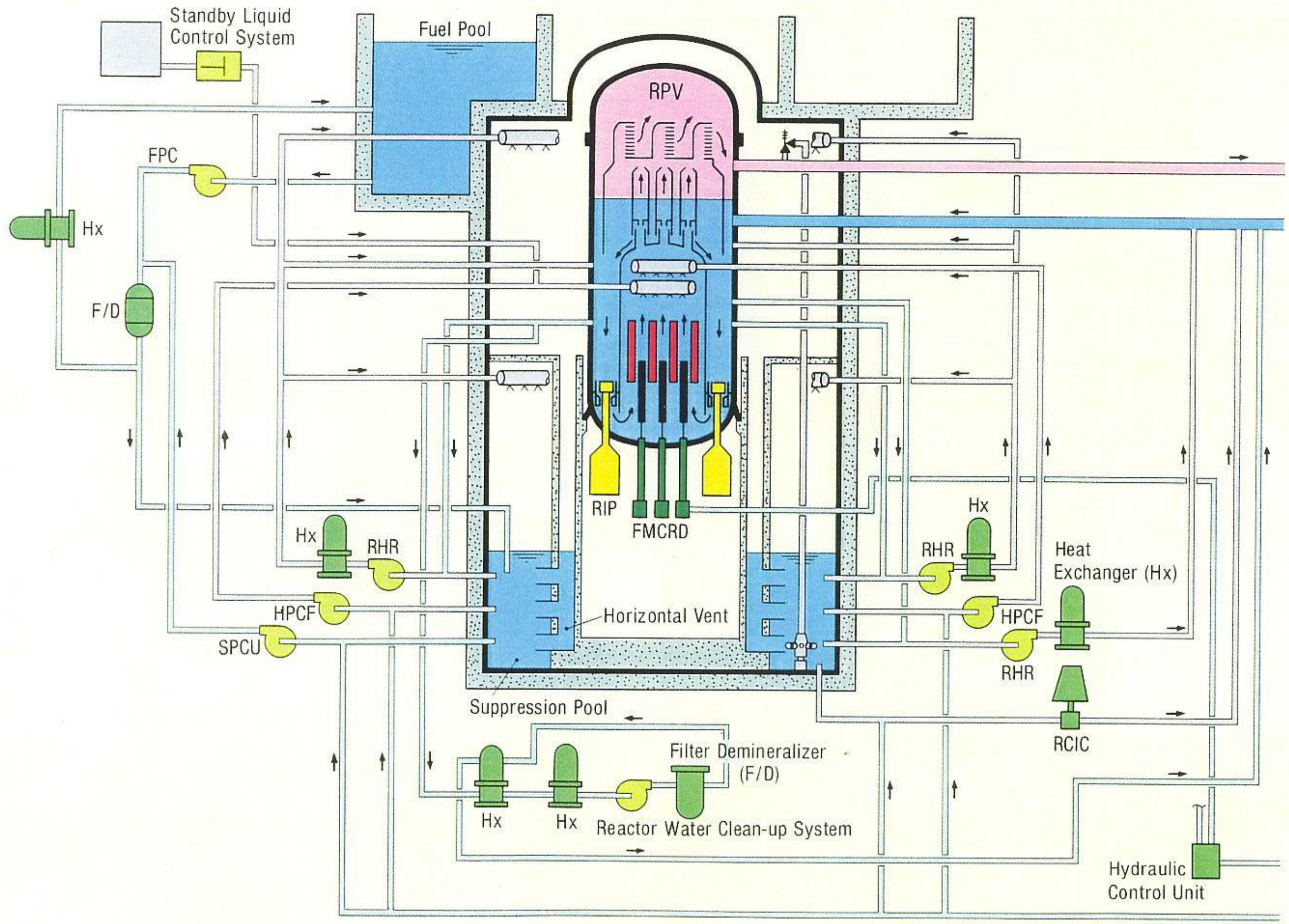
  Single Failure Criteria means that a prescribed safety function of a component is lost due to single event.

  Single Failure Criteria includes inevitable multiple failures due to single event.

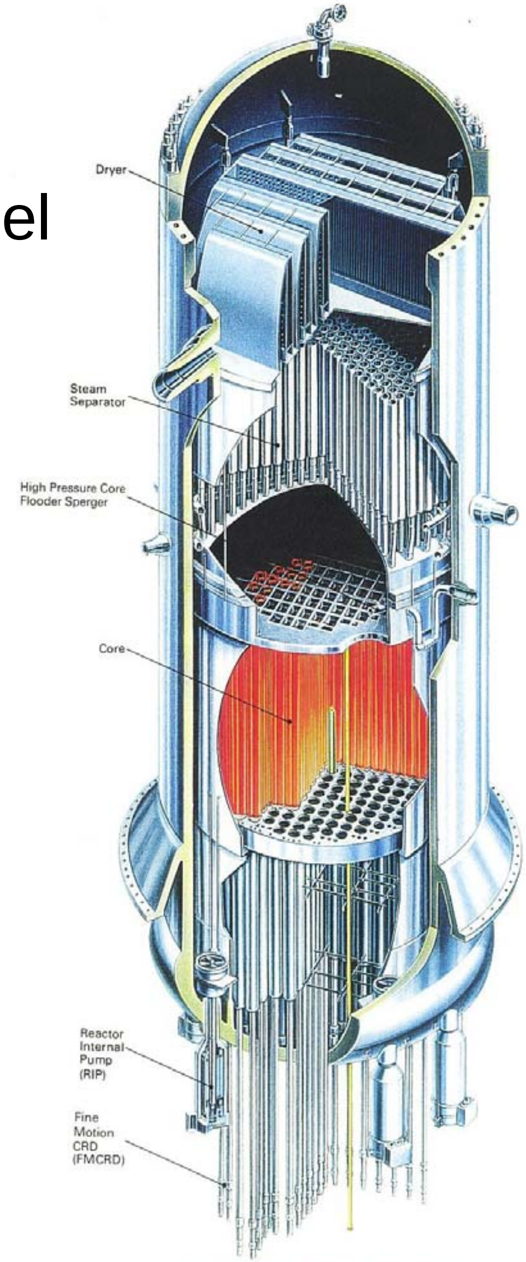
# BWR Nuclear Power Plant



# ABWR Nuclear Power Plant



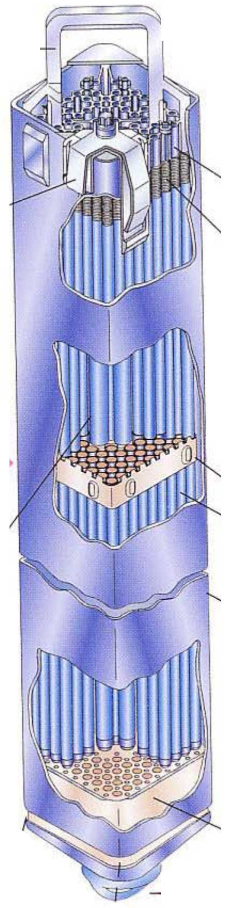
# ABWR
# Reactor Pressure Vessel



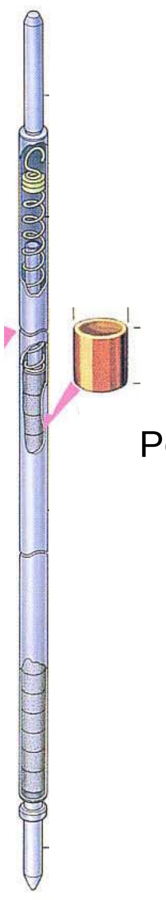

REACTOR PRESSURE VESSEL
AND INTERNALS

# Fuel Assembly

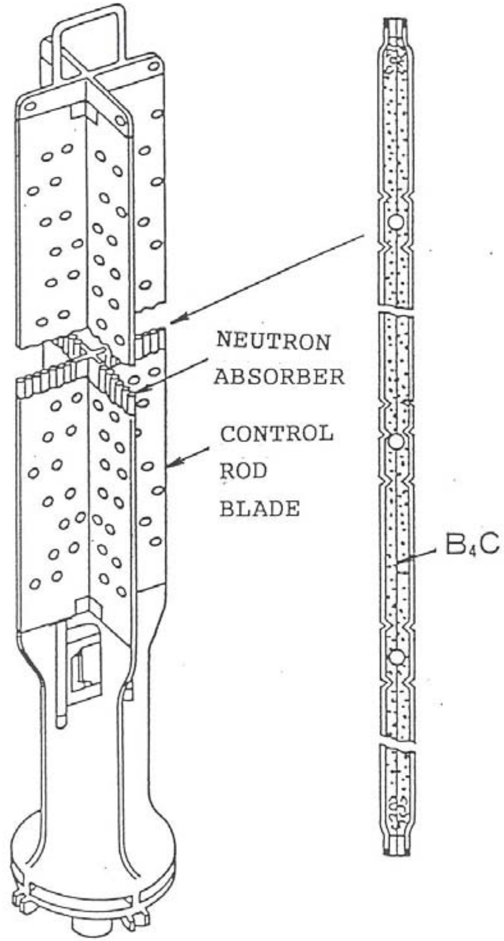
Fuel assembly



Fuel Rod

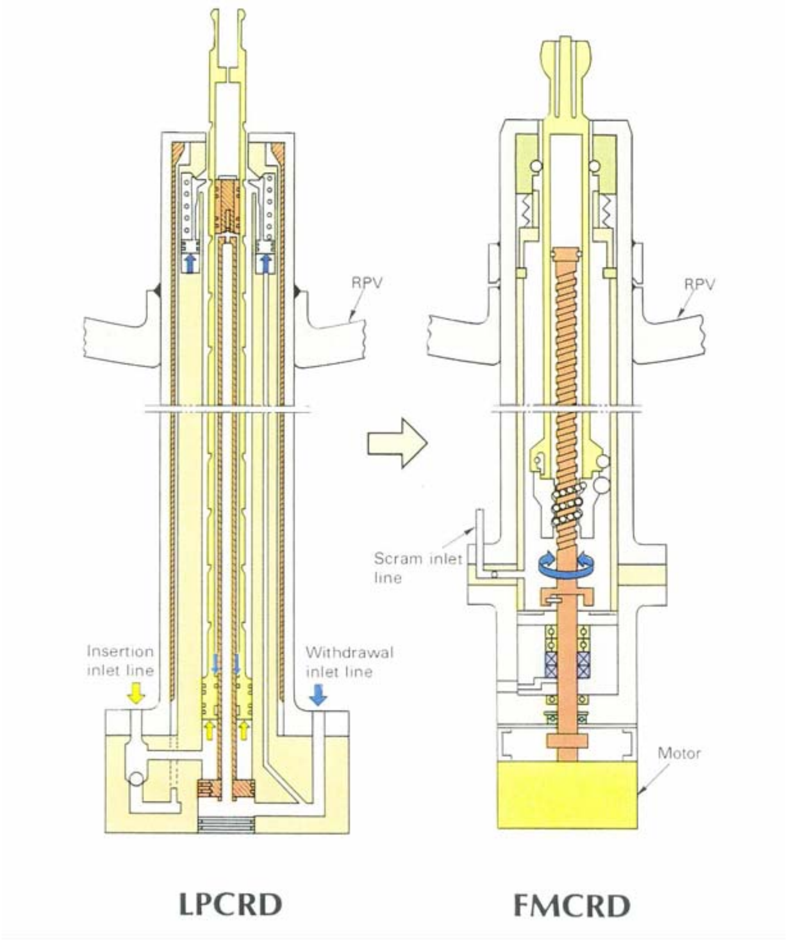


# Control Rod

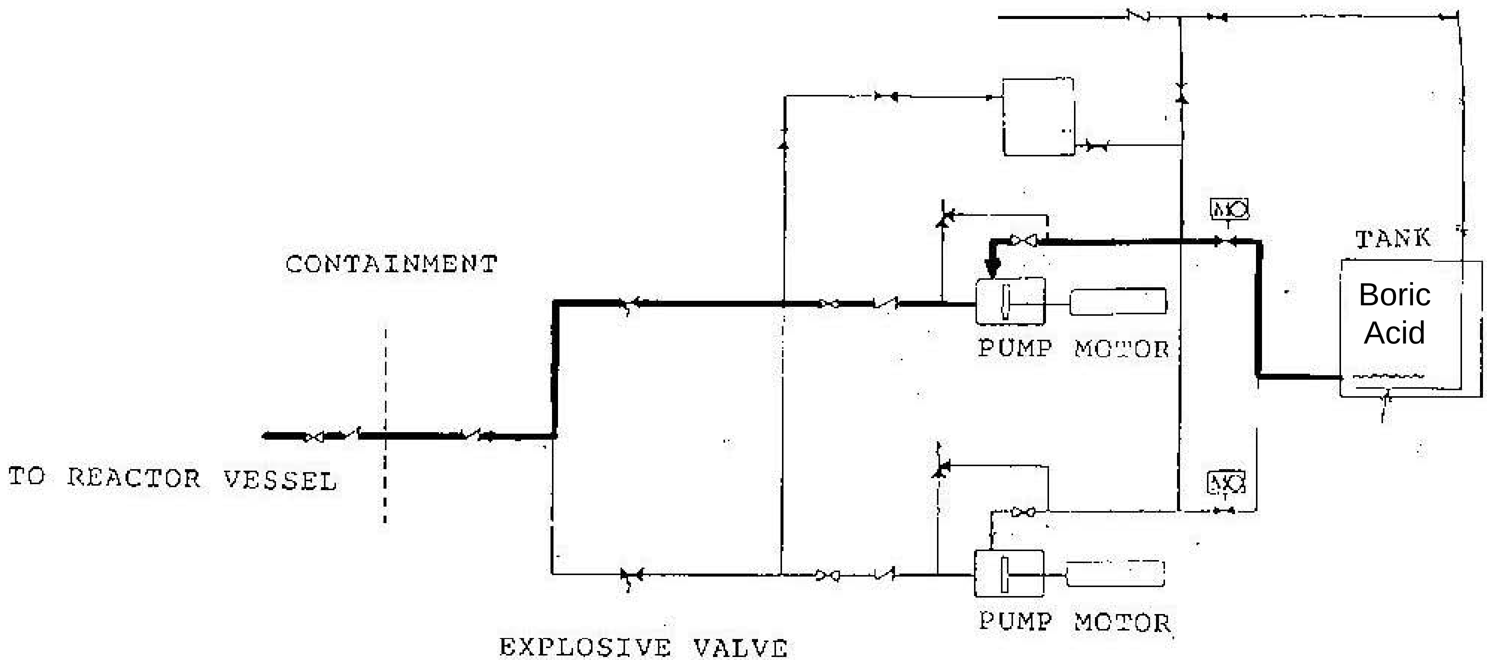


# Control Rod

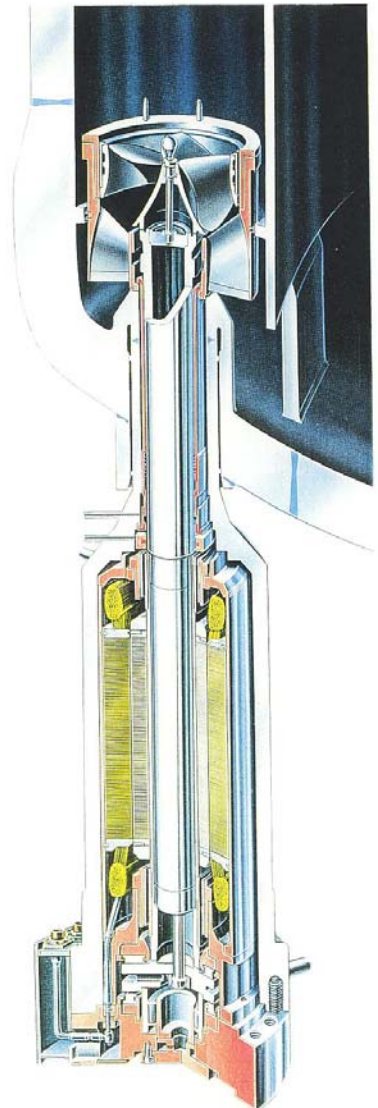
# Control Rod Drive System



# Stand By Liquid Control System



# Reactor Internal Pump



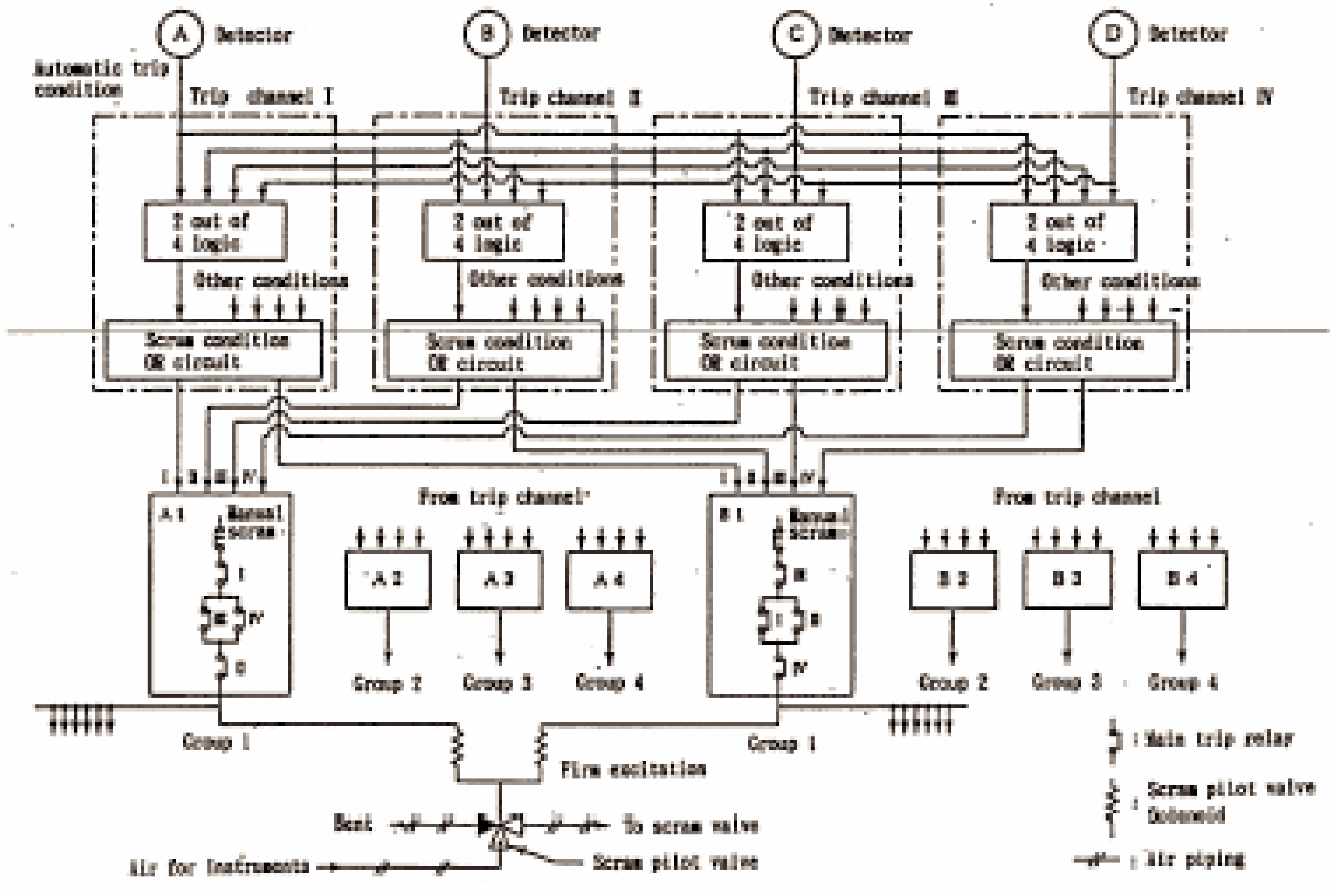
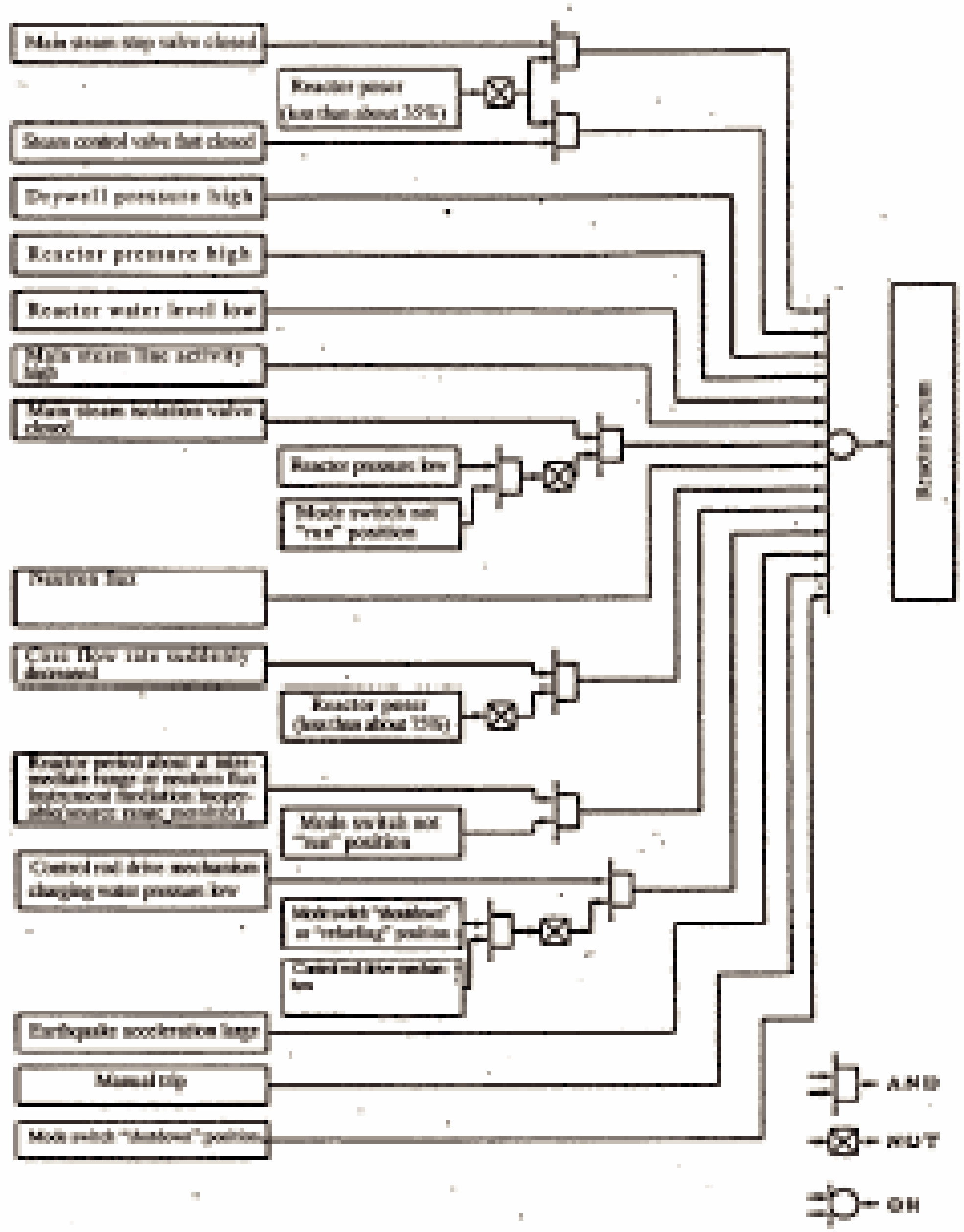



Fig.7.1 Schematic Diagram of Operating Circuit for Reactor Emergency Shutdown System

Fig.7.2 Block Diagram of Reactor Emergency Shutdown System



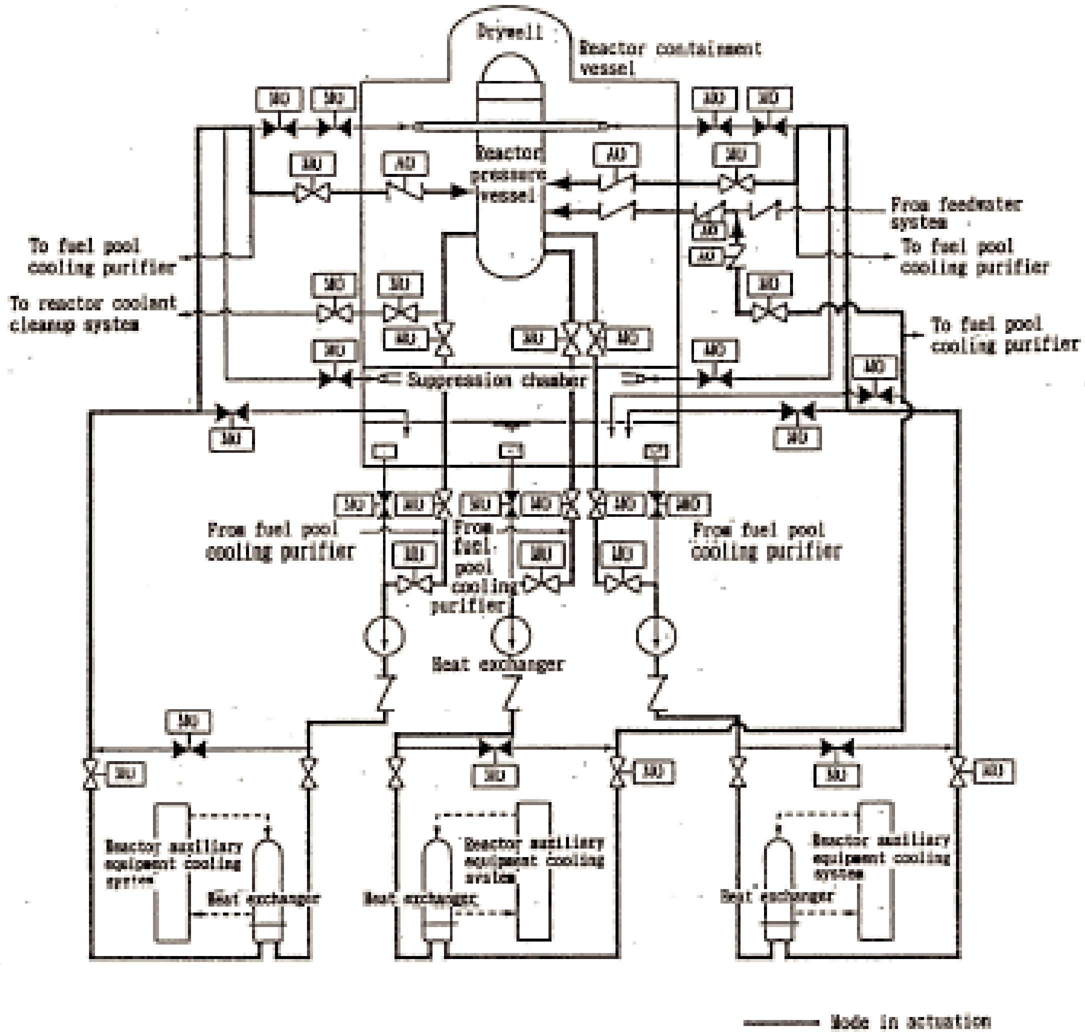



Fig.6.1 Residual Heat Removal System (Cooling Mode at Reactor Shutdown)

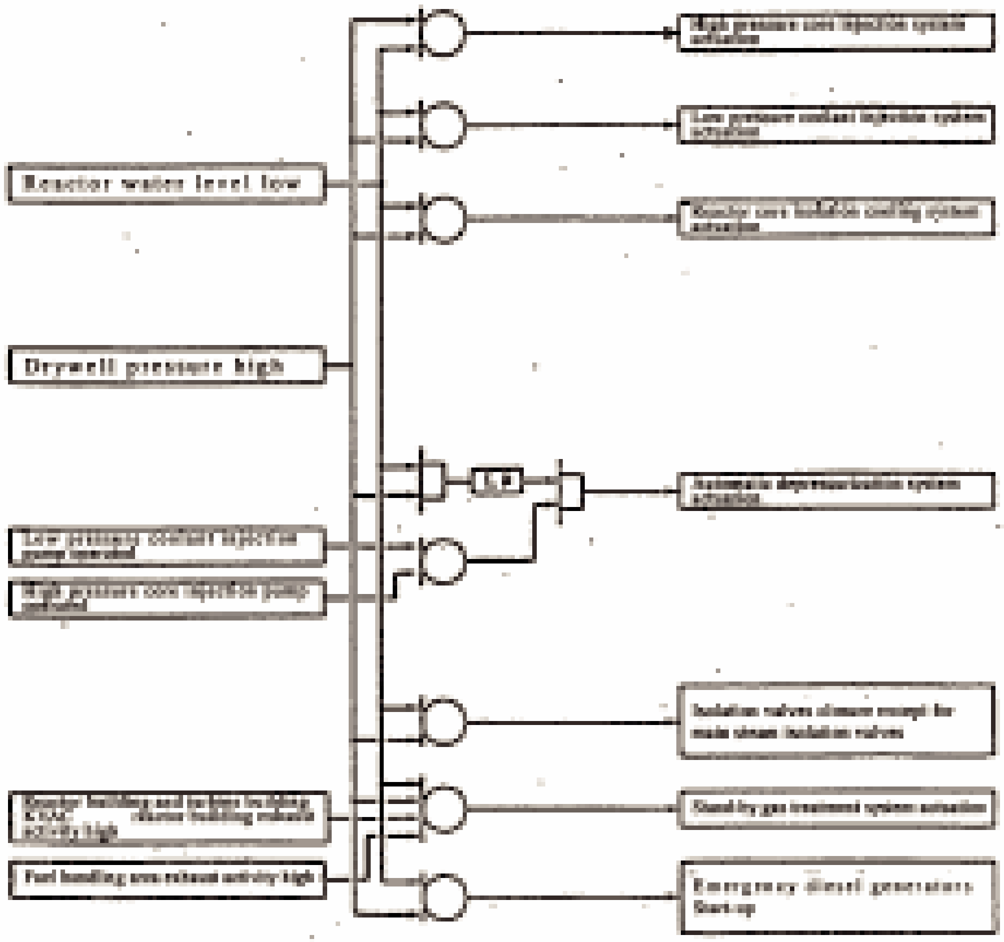
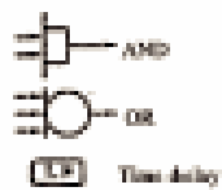
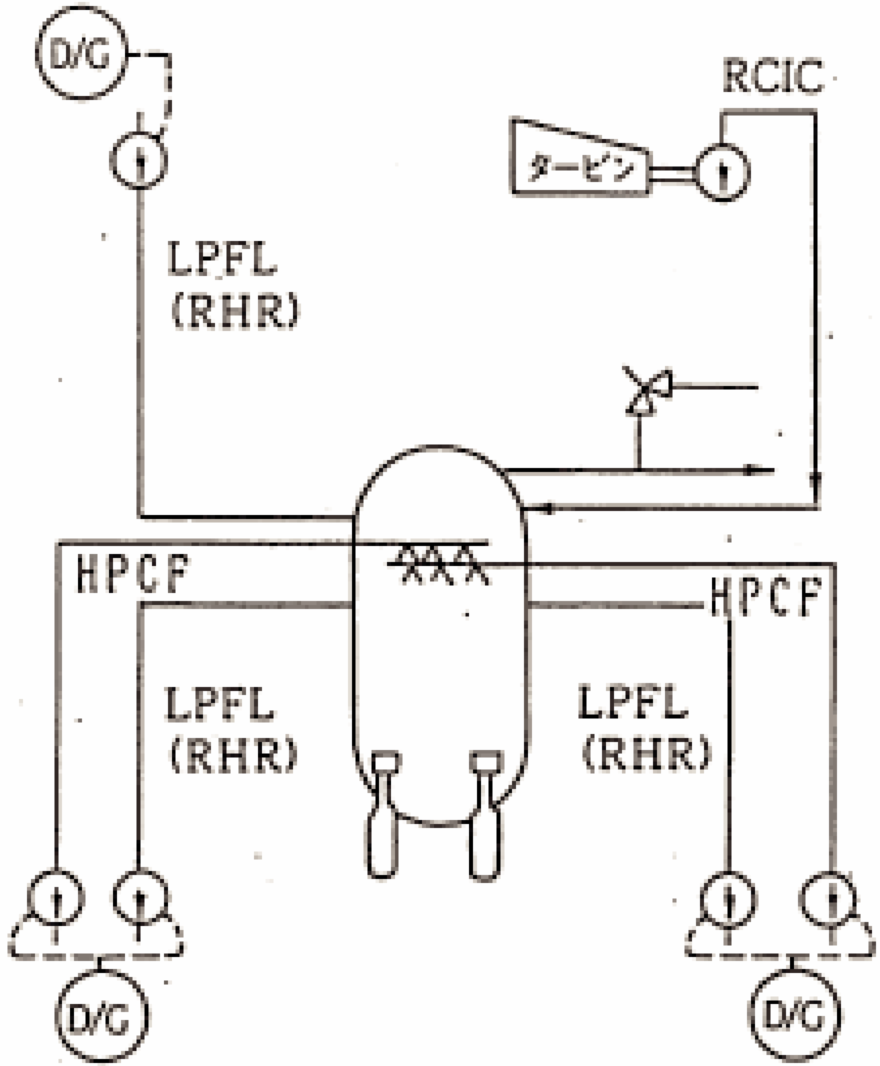


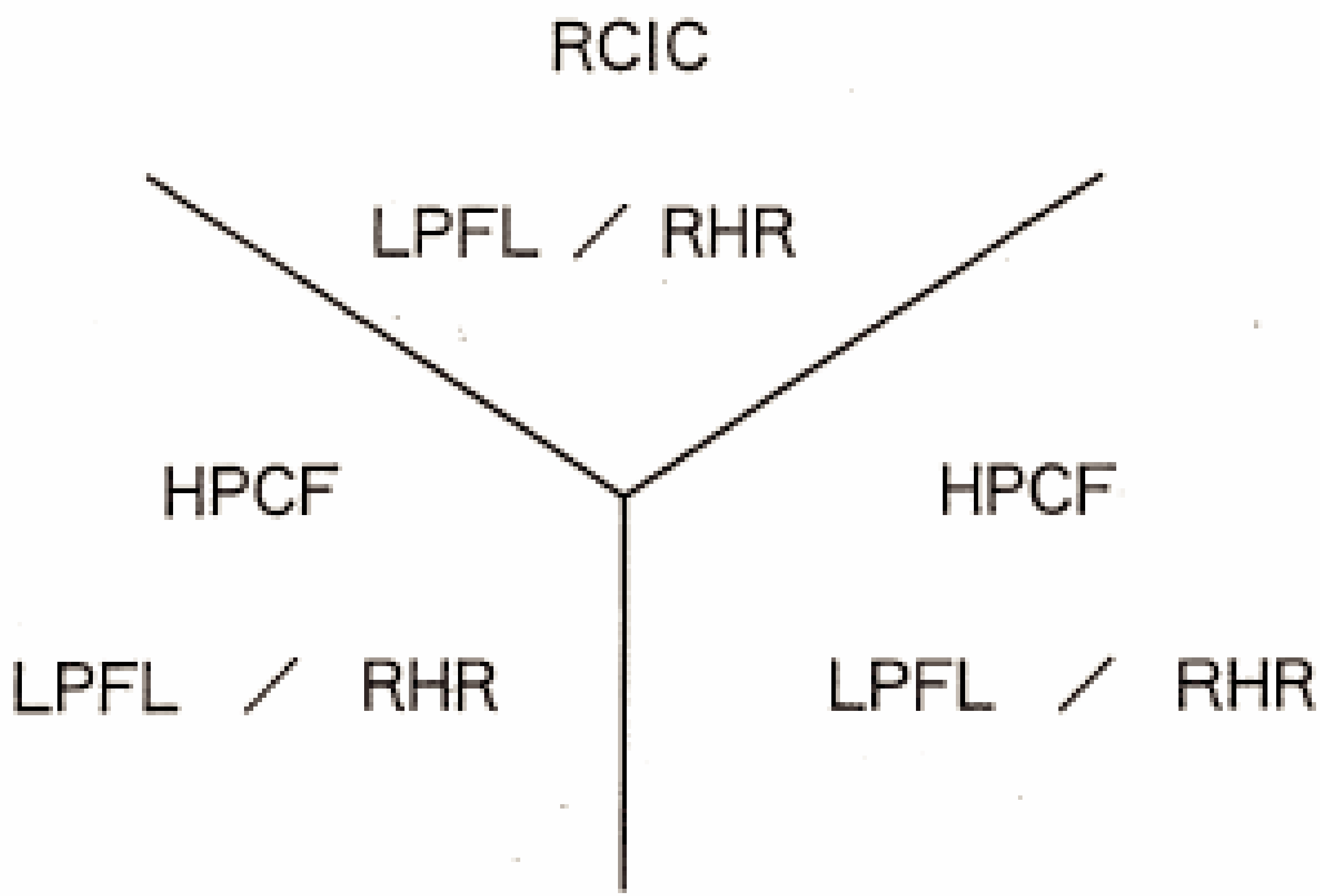

Fig.7.3 Block Diagram of Engineered Safety Feature Actuation System



Number Of Train And Its Capacity In Safety System

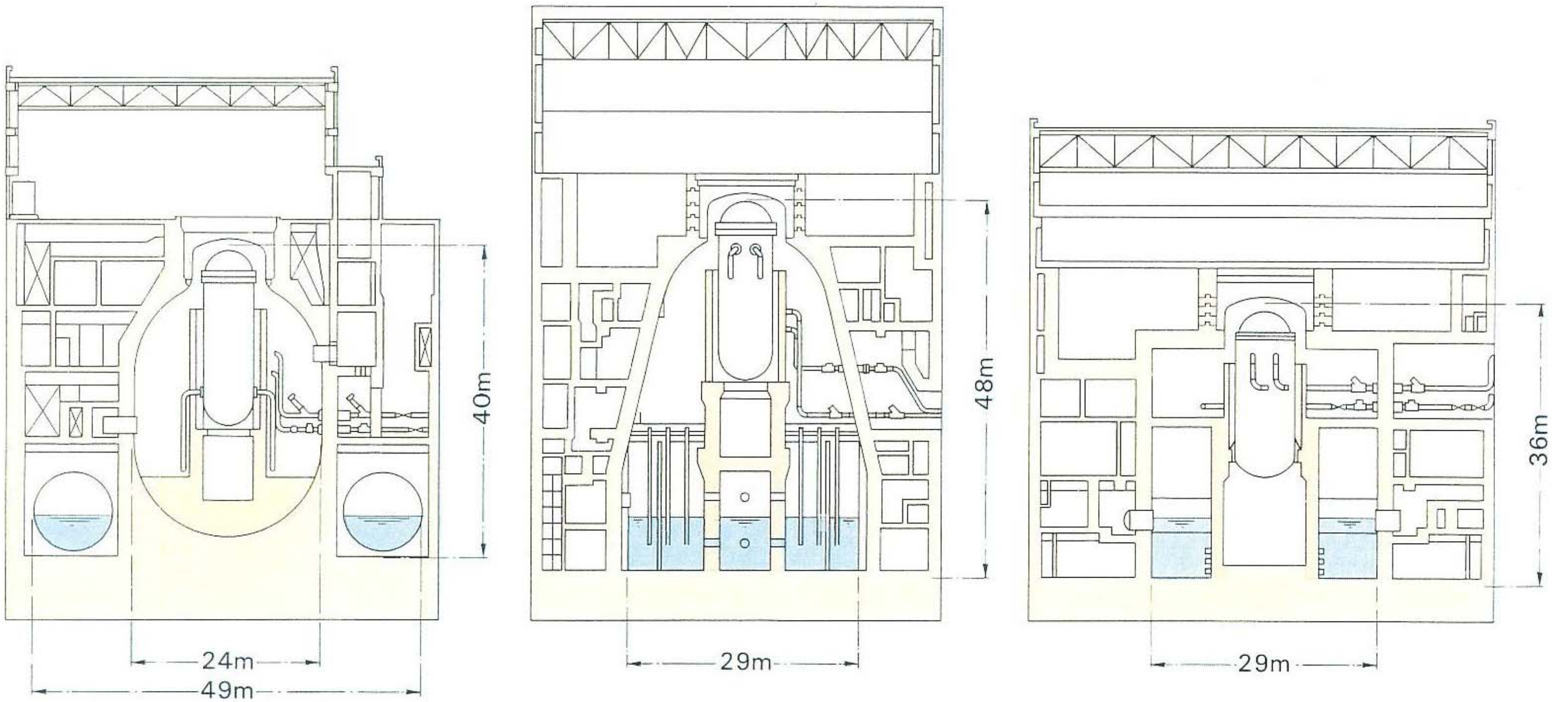
| Requirement / Capacity | N | N+1 | N+2 |
|---|---|---|---|
| | - Necessary For Normal Operation | - Same As Left<br>- Single Failure | - Same As Left<br>- Single Failure<br>- Maintenance |
| 100% for 1 Train | 1 Train 100% | 2 Train 100% + 100% | 3 Train 100% + 100% + 100% |
| 50% for 1 Train | 2 Train 50% + 50% | 3 Train 50% + 50% + 50% | 4 Train 50% + 50% + 50% + 50% |
| 33% for 1 Train | 3 Train 33% + 33% + 33% | 4 Train 33% + 33% + 33% + 33% | 5 Train 33% + 33% + 33% + 33% + 33% |


D/G
RCIC
タービン
LPFL
(RHR)
HPCF
HPCF
LPFL
(RHR)
LPFL
(RHR)
D/G
D/G




3-Division In ABWR ECCS

# BWR Reactor Containment




IMPROVED MARK-I
(1100 MWe Class)

IMPROVED MARK-II
(1100 MWe Class)

ABWR
(1350 MWe Class)

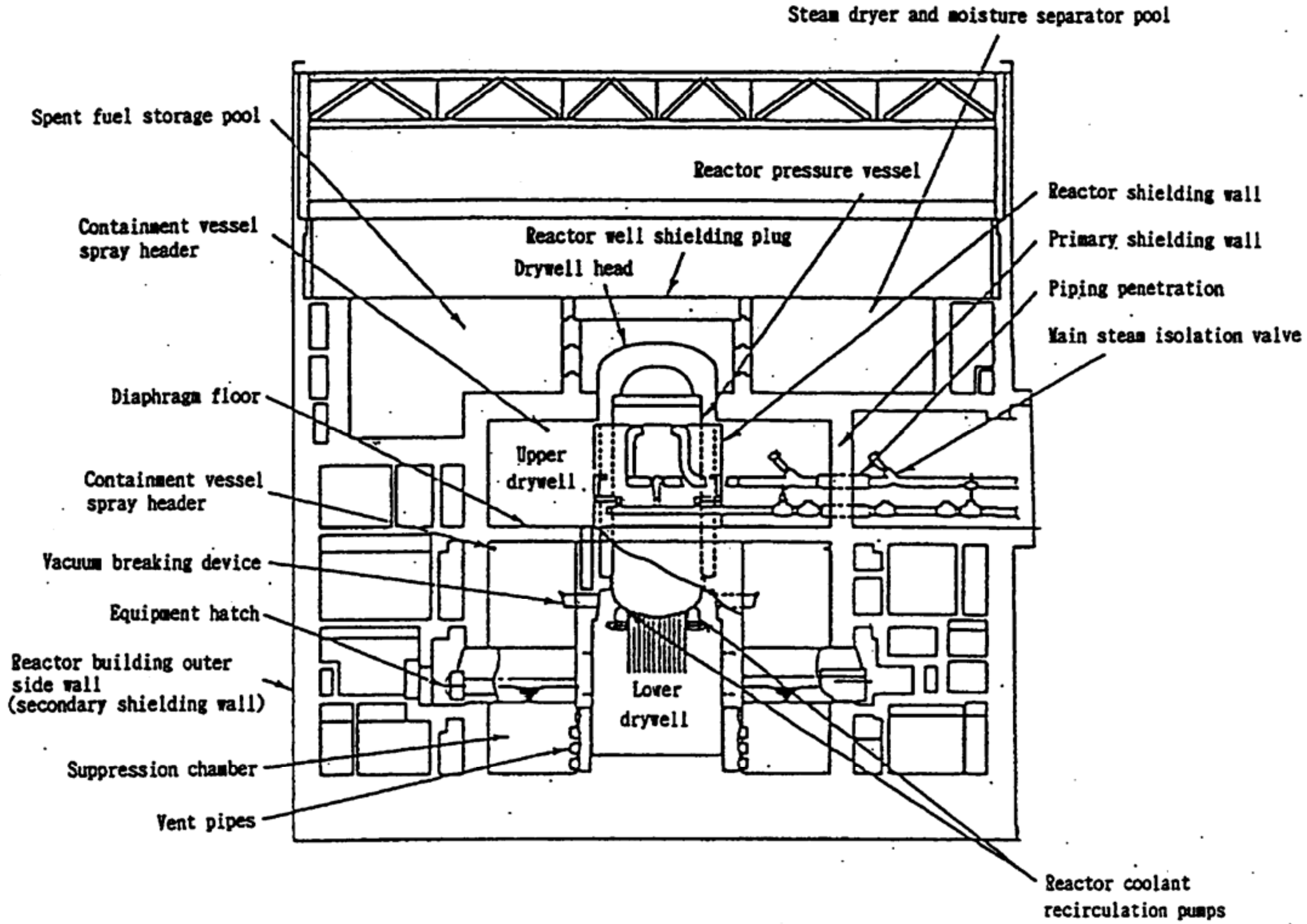



Fig.5.1 Schematic Structure of Reactor Containment Facility (ABWR)

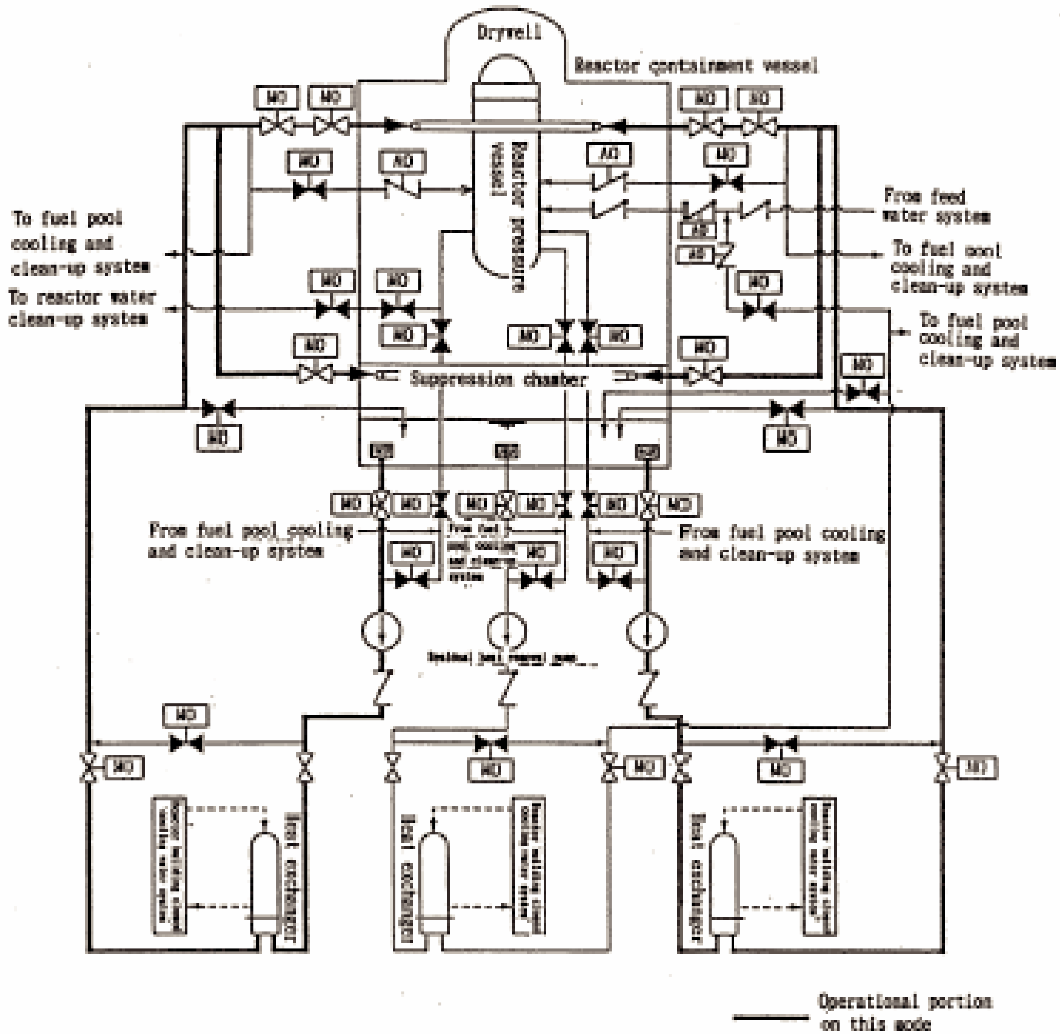



Fig.5.2 Containment Vessel Spray System (RHR system at containment vessel spray cooling mode operation)

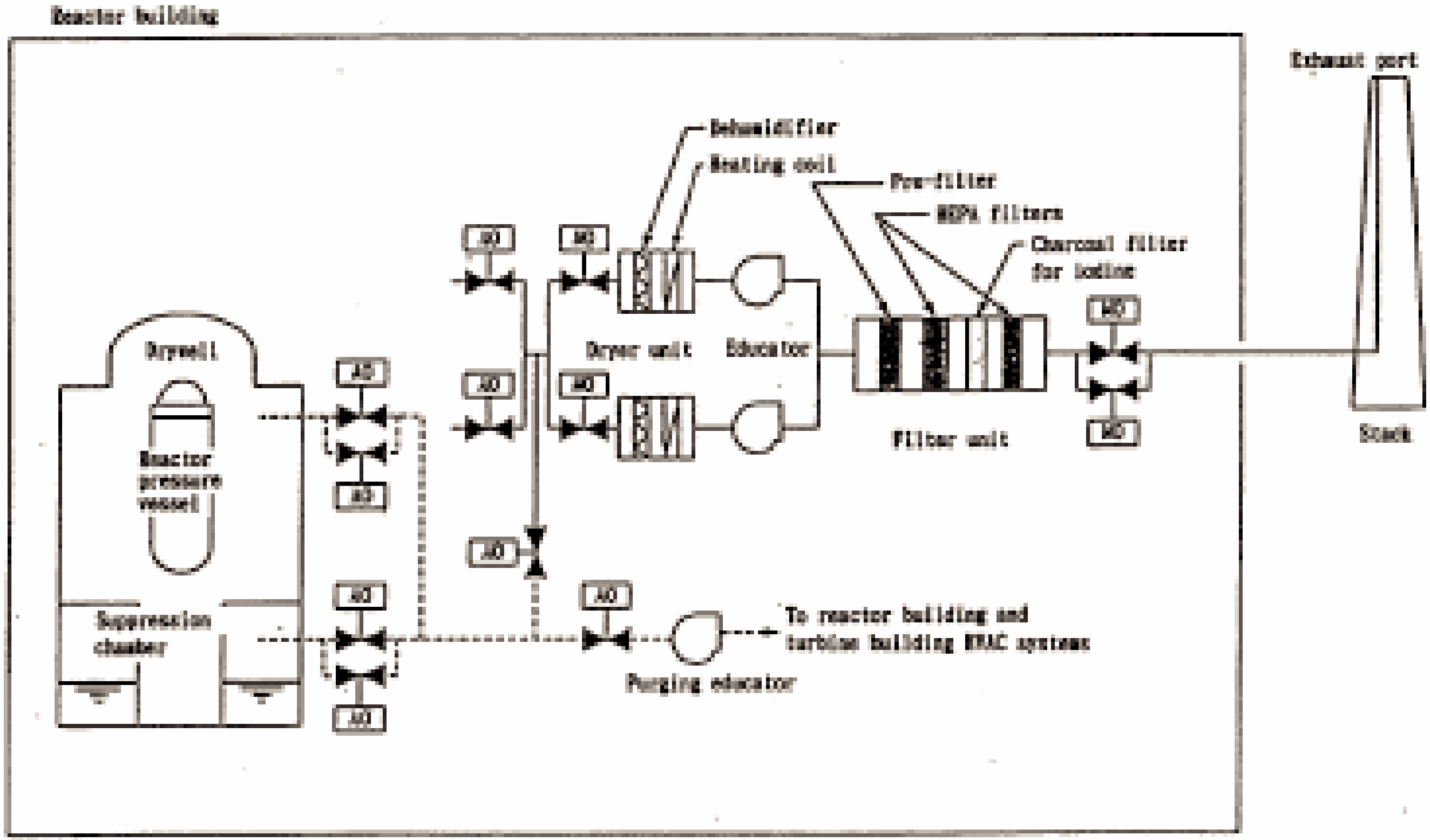



Fig.5.4 Schematic Flow Diagram of Emergency Gas Treatment System

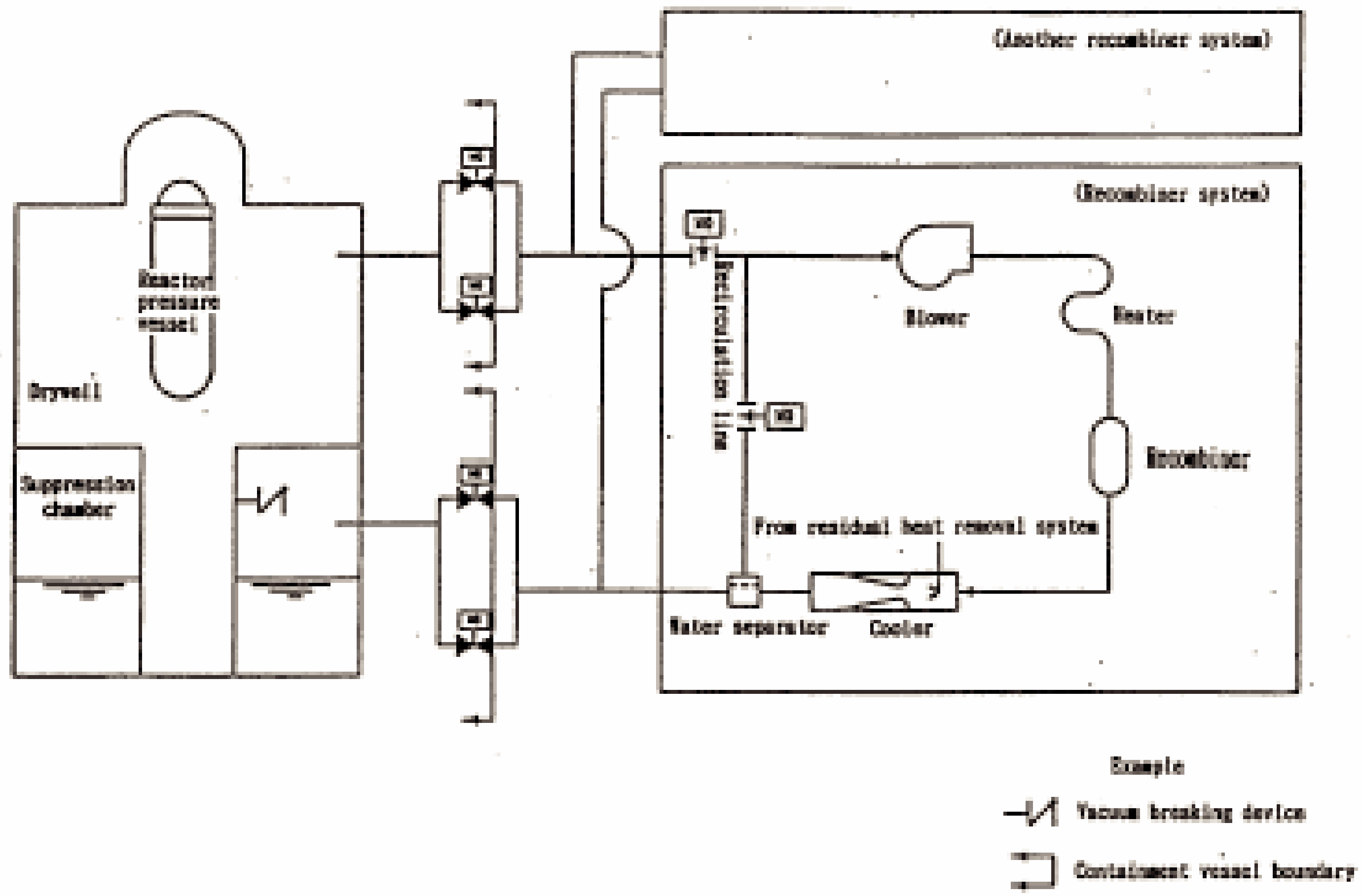



Fig.5.3 Schematic Flow Diagram of Flammability Control System