I S P R A - SEMINAR

Thermohydraulic Problems Related to PWR Safety

Introduction to PWR Safety - Part I: Design Basis Accidents

by F. Mayinger

1. The Primary Cooling System of a PWR

There are several types of nuclear reactors which can be subdivided according to its cooling or heat transfer medium - gas, light water, liquid metal - or with respect to its neutron sprectrum - fast reactors and thermal reactors. For commercial electricity generation the so-called "light water reactor" has become the standard type for commercial nuclear power stations. In this reactor type the heat generated by the fission process is absorbed and transported by normal demineralized water, and the same water is also used for moderating the neutrons from the high energy level to the thermal one.

Depending whether the water in the fission area of the reactor is partially evaporated or not, the reactor is called a "boiling water reactor" (BWR) or a "pressurized water reactor" (PWR). The energy conversion from heat to mechanical or electrical energy is the same as in conventional coal or oil fired power stations, i.e. steam is feeding a turbine which drives an electrical generator. In the case of the boiling water reactor the steam produced in the reactor immediately operatrs the turbine. In the pressurized water reactor the water heated up in the fission area delivers its heat in a heat exchanger to a second water system in which evaporation takes place and this vapour drives the turbine. That is why one speaks in the case of a boiling water reactor of a "single loop system" and in case of the pressurized water reactor of a "double loop system". The cooling system which incorporates the fission area is called the "primary system".

Here we are discussing the Pressurized Water Reactor (PWR) only.

As mentioned already, the pressurized water reactor (PWR) has a primary and a secondary system. Both are linked together via a heat exchanging device, which is called the steam generator. The primary circuit is a simple heat transport system in which the thermal energy produced in the fission area is ansported via circulation pumps to heat sinks, i.e. to the steam generators. To get a reasonable thermal efficiency the heat must not be produced at too low temperatures which - due to the thermodynamic properties of the water - means that there has to be a certain pressure, to avoid evaporation in the primary circuit. The usual pressure and temperature conditions in PWRs are 140 to 160 bar and 300 to 340°C. These thermodynamic conditions are in many respects an optimum or a compromise, especially concerning thermal efficiency, corrosion and costs of investment. The high pressure in the primary system means that there has to be a very expensive construction of apparatus and pipe-lines.

The fission material where the heat is produced is pressed into small pellets of about 10 mm diameter, which are filled into tubes and these tubes are assembled to so-called "fuel elements". An arrangement of a certain number of fuel elements is then called the "core". The core again is surrounded by a thick-walled pressure vessel which is connected via pipe-lines with the steam generators. The water transport through these pipe-lines from the pressure vessel with the core in it to the steam generators and back is sustained by a circulating pump. This arrangement of pressure vessel, circulating pump, pipe-lines and steam generator we call a "primary loop". There are up to four primary loops in a pressurized water reactor, all four connected to one pressure vessel containing the core. Two of these loops can be seen in Fig.1. The reason for subdividing the primary circuit into four loops is: primarily, to reduce the size of the steam generating apparatus, and secondarily, to get a higher availability for the cooling circuit, especially with respect to pump failures. Modern PWRs, producing an electrical power of 900 or 1300 MW, consist of 3 or 4 "secondary loops", respectively.

During the fission process a high radioactive inventory is produced in the decay products and the hermetically closed and sealed tubes, where the fuel pellets are filled in, act as a first barrier. The second barrier against radioactive emission are the thick walls of the primary loop, mainly the pressure vessel. Finally there is a third barrier, namely the containment shell which is formed ba a spherical steel-cover of 50 to 60 m diameter with a wall thickness ot 20 to 30 mm. This steel containment - as shown in Fig.1 - again is surrounded by a concrete wall, which on its inner surface is plated with a metallic sheet. The room between the steel containment and the concrete building is kept to a lower pressure compared to the atmospheric pressure, and the air is exhausted from this room via a filtering system of very high efficiency, which guarantees that the radioactive impact on the environment of the nuclear power station is less than 1 mrem/a during normal operation. This is negligible compared to the natural radioactivity which lies in the order of 100 to 200 mrem/a, depending on the height above sea level and on the natural radioactive sources in the soil.

The cooling water enters the pressure vessel, as shown in Fig.2, through nozzles - there are, corresponding to the number of primary loops, three or four of them - and then the water flows through an annular downcomer to the lower plenum, from where it enters the fuel elements of the core. Flowing through the fuel elements it is heated up and it leaves the pressure vessel through the nozzles in the upper plenum for the steam generators. The pipe-lines carrying the heated up water from the pressure vessel to the steam generator are called the "hot legs". The circulating pumps are located in the "cold legs", which contain the water flowing back from the steam generator to the pressure vessel after having been cooled down by about 10 to 30 K.

In the reactor of a large nuclear power station with about 1300 MW there is an inventory of approximately 100 t uranium-dioxide (UO_2). To carry the heavy load of this fuel there is

a grid support plate and a core support construction in the lower plenum of the pressure vessel, as shown in Fig.2. At its upper ends the fuel elements are fixed in the upper grid plate.

The pressure vessel for a large power station has a diameter of approximately 5 m, with a wall thickness varying between 150 and 450 mm. The wall thickness of the cylindrical part is 250 mm. The total height of the pressure vessel is approximately 18 m.

The hermetically sealed pipes with the fuel pellets in it - called "fuel rods" or "fuel pins" - are arranged in clusters of 15 x 15 to 17 x 17 rods in rectangular array, depending on the manufacturing design, as shown in Fig.3.

For controlling means and for shut down of the reactor, neutron absorbing material has to be brought into the fuel elements, which - in case of pressurized water reactors - is arranged in form of slender rods, as shown in Fig.3. To allow these absorber rods to penetrate into the fuel element, several positions in the rectangular array are not taken by fuel pins, but only have empty tubes in which the absorber pins fit in like fingers. Each bundle of the absorber fingers is connected with a thick rod which can be moved up and down through the upper cover of the pressure vessel (see Fig.2) by a control rod driving mechanism. To say it clearer, in reality there are two different driving mechanisms; one is used for controlling devices and is moving the control rods slowly and exactly up and down, and the second one is able to shoot the absorber rods very fast into the core, in case a sudden shut down is necessary.

The fuel pins are held in its radial position by grid plates, at its upper and lower ends. In commercial power plants the lengths of the fuel pins filled with pellets is approximately 4 m. This means that there have to be several devices to keep the rods in its radial position between the lower and the upper grid plate, too. These devices are called "spacers" and are arranged in a distance of approximately 0,5 m. There are more than 45.000 fuel rods in a large commercial reactor of 1.300 MW electrical power.

The design of the steam generator is - from a first point of view - very simple, as shown in Fig.4. The primary water enters the pressure vessel of the steam generator and from there, via a thick-walled grid plate, it flows through a U-tube bundle. It leaves the steam generator again through the other side of the lower plenum. Inlet and outlet part of the lower plenum of the steam generator are separated by a sheet of metal. Outside the U-tubes there is the evaporating secondary water. On its way to the nozzle at the upper end of the steam generator vessel, the vapour produced is cleaned from liquid droplets by separators and dryers. The saturated steam then flows to the turbine. To avoid corrosion on the secondary side at the bottom of the grid plate, fluid dynamic devices of different design are used by the manufacturers.

The circulating pump is of the usual design, as shown in Fig.5, having one radial wheel. The pump is driven by an electromotor, and there is a very complicated sealing of the pump shaft to avoid unallowable leakage of primary water.

The containment - as shown in Fig.1 - is not only good to prevent the escape of radioactivity to the environment during normal operation, it also keeps the whole inventory - water, steam and radioactive products - safe within the shielded area in case of a leakage of the primary system, for example, when a pipe breaks. Thus, the containment has a very important safety task, which we will discuss later.

2. Accidents and Safeguards

2.1 General Safeguard Philosophy

Accidents and incidents can be due to an internal failure in the system, or to an impact from outside. First of all, however, it has to be clearly stated that the layout and the design of all components and parts of a nuclear reactor are done under very conservative and deterministic assumptions for possible and credible failures and dangerous incidents. A very essential contribution to guarantee the safe operation of a reactor is to be seen in the measures which prevent failures in parts or components of the system, or which reduce the probability that failures occur by a very considerable amount. These measures are:

a very careful design and layout with high safety factors,
quality insurance during manufacturing and mounting,

regular and repeated tests and inspections,

verifying of important process data.

Thus an extremely high reliability of a nuclear reactor can be guaranteed. However, this does not mean that the possibility of an accident is excluded or not taken into account. This quality insurance is rather to be seen as a first step of the defence in depths against accidents and its consequences. If an accident should have happened, there are several safeguards and measures to avoid a radioactive contamination of the environment. It is custonary in conventional engineering to improve a product by experience. This is not only true for the availability and the efficiency of a machine or an apparatus but also for its reliability. This method is not practicable in nuclear engineering, as it can be understood easily. Therefore, by a detailed and careful study, all possible accidents have to be examined and the layout of the safeguards has to be in such a manner that the latter can overcome the most severe credible accident, which has to include all other minor accidents. This "engineering judgement" - as it is called - has to include all possible and conceivable failures of the system.

However, also the safety devices may fail and, therefore, they are usually available in a redundant number; that means, even when only one device is necessary to overcome the accident, there are three or four of them to reduce its unavailability to a negligible figure. The fundamental task in nuclear safety is to prevent that after an accident radioactivity can escape to the environment in an unallowable amount. As mentioned, there are three barriers to avoid the escape, namely the tubes in which the pellets are canned, the pipes and pressure vessels of the primary system, and the containment shell. If one of these barriers is penetrated or destroyed, the others - or at least one - has to withstand. How this is provided, or which safeguards have to be taken, is depending on the nature of the accident.

In case of a transient or an accident, safety measures have to guarantee that

- the reactor is safely shut down and no power excursion can take place,
- the reactor core can be cooled sufficiently and for a long period within tolerable temperature limits and
- radioisotopes cannot escape into the environment in an unallowable amount.

Safety installations guaranteeing these conditions are:

a) the reactor scram system which effects a fast shut-down of the reactor and, by this, prevents an unallowable power excursion;
b) the emergency cooling and decay heat removal system, which prevents a superheating of the core, due to decay heat production, when the reactor is depressurized;
c) the emergency feed water system, acting as a heat removal system in cases of accidents, if the primary system is still under pressure, however, the turbine and the condenser fail as heat sinks;
d) the safety isolation system, preventing that radioactivity escapes into the environment outside of the containment;

e) the safe emergency power system - mainly Diesel-generators - which is needed to supply the above mentioned safety systems with electrical energy, in cases when power supply from outside fails completely.

As long as these safety systems act properly, any accident can be governed without consequences for the environment. However, as mentioned before, it is much more important to prevent such accidents instead of putting the emphasis of safety activities and safety measures to mitigate its consequences. For a safe and reliable operation of nuclear power plants, therefore, we have to take in account four different kinds of measures which are initiated and performed by different systems.

a) The normal operation system:
This system contains all measuring- and controlling devices and apparatus being necessary for the operation of the plant, not assuming an incident or accident.

b) The safeguard system:
It contains all components having the task to protect the plant or parts of it under unnatural operating conditions from damage and destroyment.

c) Safety and emergency systems,
having to protect the environment against damage:
Emergency systems have to fulfil its task after failure of all operating- and safeguard systems.

d) Organizing measures in case of a severe accident by the public authorities to minimize the consequences, for example, in the case of a core melting.

A failure of a component in the operating system may create a situation and a deviation from the normal operating conditions, which cannot be mastered by the normal controlling system. In this case the safeguard systems would become active and would initiate measures to protect the components of the primary and secondary system against overstressing. So, for example, the turbine will be switched off or the safety valves prevent an overpressure of the primary or the secondary system.

However, there may be also wrong signals from the safeguard systems, initiating an unnecessary safety procedure which, by itself, may produce a severe transient or even an accident situation.
To eliminate wrong safeguard signals as much as possible, the so-called "2 of 3 or 2 of 4 switching system" is used. This means: Only if 2 of 3 or 4 sensors report an unallowable situation - being outside of the normal operating conditions to a certain extent - the safeguard system is activated.

2.2 Accidents from Outside

Possibilities for accidents from outside are

- chemical explosions,
- airplane crash,
- earthquake and
- sabotage.

The probability for an airplane crash is higher from military aircrafts than from civil ones. At present the phantom fighter would give the highest momentum and impact on a building when crashing down. From a strategic point of view there is a tendency in all defence ministries, not to develop heavier airplanes having the same velocity, but to develop lighter ones in future. Therefore, the layout of the concrete wall around the containment of the reactor has to withstand the crash of a phantom fighter coming down with a velocity of almost 800 km/h. Taking into account the design of the aircraft, mainly of a jet engine, a time-depending dynamic load results, as shown in Fig.6.

The maximum load amounts up to 11.000 Mp and the total impact time is approximately 70 ms. That load makes necessary a wall thickness of a strongly reinforced concrete between 2 and 1,3 m, from the bottom to the top of the reactor building, respectively. This is also the layout of modern reactor building in the Federal Republic of Germany.

With chemical explosions the question of layout becomes a little more difficult. Chemical explosions can result from ship accidents, when a tanker filled with explosive gas or evaporating liquids is involved in it. The amount of explosive gas which becomes free is depending on the largest size of vessels shipping up and down the river where the nuclear power station is situated. The present situation makes it reasonable to assume a cloud of gas having a diameter of 50 m, which can be drifted to the nuclear power station until it is adjacent to the reactor building and ignited by any means. The pressure resulting from the following explosion is depending on the velocity of the flame. This velocity is a function of the gas, of the air/gas concentration and of the turbulence in the flame. Theoretical calculations - done under pessimistic assumptions - gave a maximum pressure in the forward-travelling wave of 0,3 bar and in the reflected wave of 0,45 bar. Higher pressure would result if the explosion could change into a detonation. This, however, from a theoretical point of view can be excluded in the free atmosphere. Nevertheless, in the German licensing rules issued by the Minister of Inner Affairs, a formula for explosion loads is used, which is based on a detonative reaction in the gas-cloud.

One can object that this is a pure theoretical result, not verified by tests. There were several accidents resulting from chemical explosions, in chemical factories and in goods stations, which caused serious damage. Evaluating the extent and the nature of the damage and knowing the amount of exploded gas, one can recalculate the pressure of the explosion wave. An evaluation of such accidents gave the pressure course as presented in Fig.7. In this figure there is plotted the maximum pressure in the explosion wave versus the distance from the center of the ignited cloud, divided by the exploded mass. Certainly, there is a wide scattering of the data which is due to the difficulty of the evaluation method, however, it can be seen clearly that the assumption of 0,45 bar maximum pressure in the explosion wave is conservative. This a clear confirmation of the above mentioned theory.

The assumptions for earthquake loads are depending on the place where the power station is situated. There are areas of high earthquake activities - like the upper part of the Rhein-river - and others, where an earthquake never was reported. As basis for the layout, usually the strongest earthquake is taken being historically known for that area. In general one defines two categories for earthquake layout: The lower one is called the "operational layout", which means, normal operation systems have to withstand it. The higher one is called "safety layout", against which all emergency devices and safeguards - including the primary system and the containment - have to withstand. In active zones of the FRG an intensity of 7 in the Richter-scale is assumed for this safety layout. The layout against earthquake is a question of civil engineering and should not be discussed here in detail.

Measures against sabotage primarily have to prevent that saboteurs can come in from outside. However, in addition emergency devices are available double and threefold and are situated in far distance from each other, which means that if one of them would be destroyed, another one could take its duties automatically.

2.3 Accidents from Inside

An accident from inside can result due to a failure in the primary system, e.g. in the energy supply for the circulating pumps, or a crack or break in a pipe or in the pressure vessel. From the safety point of view we have to distinguish between accidents after which the primary system is intact - e.g. the mentioned pump goes down - and others where the primary system fails. The first category is not a safety problem from the environmental point of view because the radioactivity remains safe and closed in the primary system, as long as there is not an overpressurization resulting from this accident leading to a break.

Careful studies have shown that the layout of nuclear power stations is such that a pump failure - may be due to lack of energy supply or due to a mechanical damage in the pump or in its motor - does not result in an overpressurization and there is no danger for the fuel pins, which means that the radioactivity stays enclosed in the fuel canning. One can argue that after a failure in the pump also the control rod mechanism - which has to shut down the reactor - may fail. This is extremely improbable indeed, however, even if this would be the case, due to temperature rise and evaporation of the water, the neutron production would decrease tremendously, which means that the reactor is shut down automatically for the moment and then a second shut-down mechanism becomes active by injecting boric acid acting as an absorber. The power excursion and overpressurization in such a hypothetical accident is lying within the layout-limit, which means that it would not result in a disruption of the primary system. This accident, i.e. when the fast shut-down by the control rod mechanisms - the scram - fails, is called "anticipated transients without scram (ATWS)". There are other possibilities for ATWS which - due to lack of time - cannot be discussed here in detail. Studies have shown, however, that they are mastered by the primary system and the other safety devices.

The most serious accident is the loss of coolant in the primary system, initiated by a break in any pipe-line or in any other component of the primary system including the pressure vessel. Naturally, the probability of such a damage is kept as small as possible by very diligent material testing during fabrication and by periodically repeated tests, as mentioned before. However, it has to be taken into account as the "Maximum Design Basis Accident (MDBA)".

The fluid escaping out of the primary system is, certainly, safely kept within the containment, however, the fuel elements producing decay heat also after a scram have lost its coolant. This decay heat production is between 7% and 1%, depending on the time after the accident initiated. If the cooling effect cannot be reinstalled as soon as possible, serious damages may happen to the fuel elements and a core melting process could start. To prevent this is the task of the emergency core cooling system.

Naturally, the decay heat has also to be removed after other accidents or incidents, when the reactor lost its main heat sink - the turbine and the condenser - due to any reason. As long as the primary system is intact there is another cooling system, the so-called "feed water system" for heat removal out of a pressurized water reactor, which will be discussed in chapter 3. In the boiling water reactor the mentioned water inventory in the containment is then used as heat sink by blowing steam from the pressure vessel into this pool, as mentioned before.

In case of a break in the primary system - i.e. after a MDBA - one has to be completely sure that the containment is hermetically sealed and tight. A damage to the containment wall could result from pipe-lines which are strongly moved, due to the flow momentum of the jet stream at the break. Special devices and missile protections are, therefore, installed in the containment.

3. Emergency Cooling and Decay Heat Removal Systems

3.1 Emergency Core Cooling System

The event of the loss-of-coolant-accident is, in some respect, quite similar for all water-cooled reactors, i.e. for pressurized and for boiling water reactors. This is valid for the decay heat production after a scram and for the physical laws of two-phase flow and heat transfer during "blowdown", as the escape of the primary fluid out of the primary system into the containment is called. During the emergency-core-cooling-accident not only a core melting has to be avoided; far before this the temperature of the fuel elements has to be kept in such a safe boundary that no serious damage of the fuel rod cladding - which is made out of zircaloy - can occur, in order to prevent a not admissible increase of the radioactivity in the containment. Zirkaloy cladding loses its mechanical firmness at higher temperatures and the pressure inside the fuel rods, caused by gaseous fission products, can lead to a ballooning or to a bursting of the cladding. Furthermore, at higher temperatures there is an exothermal chemical reaction between zirconium and water, oxidizing the zirconium and making hydrogen free. If the hydrogen concentration exceeds a certain limit in the containment or in parts of it an explosion may occur.

Claiming the integrity of the fuel elements and fuel rods as far as possible after a loss-os-coolant-accident, criteria had to be fixed which should not be exceeded. These criteria are

1. the maximum zirconium cladding temperature must not exceed 1200°C,
2. 1% of the zirconium being present in the reactor pressure vessel may undergo the zirconium/water reaction in maximum,
3. maximal 17% of the cladding wall thickness may be oxidized due to the zirconium/water reaction, and
4. the fuel elements have to be reliably cooled by an emergency core cooling system for a sufficient time.

From the condition of a vast integrity of the fuel rod cladding during and after the loss-os-coolant-accident, simply the demands for the rundown of the emergency cooling and for the emergency core cooling system can be derived. Unallowable temperatures of the fuel rods and of the zircon cladding can only be prevented if each of the following demands is fulfilled:

1. It has to be guaranteed that after the loss of coolant new coolant reaches unrestricted all parts of the reactor core.
2. The heat transfer conditions between cladding and coolant have to be sufficiently good.
3. The coolant flow loaded with decay heat must not be prevented from leaving the core in order to permit new cold fluid entering the core, and
4. the technical equipment for the emergency core cooling has to supply the cooling fluid in time and to a sufficient amount for any long time.

After the break of a main cooling pipe the pressure in the pressure vessel falls down very rapidly. Especially in a pressurized water reactor with its subcooled conditions the temporal pressure gradient is very large at the beginning, due to the fact that already the smallest amount of leaking water brings the system pressure down from 160 bar to saturation pressure. The core structure and the primary system have to withstand the forces which are induced by this pressure gradient, in order to guarantee the core configuration in such a condition that the control rods can fall in, the fuel rods can be cooled and the cooling system is as effective as possible.

Depending on the area and the position of the break, the conditions during the blowdown may vary considerably. The emergency core cooling system has to work under all of these conditions and has to supply cooling fluid in a sufficient amount and in time, giving the possibility to overcome the whole spectrum of possible leaks including very small leaks without great pressure reduction.

For overcoming an accident with a large leak, a high water amount at low pressure must be supplied by the emergency core cooling system, and for one with a small leak a small flow rate but a high pressure is necessary. These different conditions depending on the area and the position of the leak, led to a development of an emergency core cooling system which possesses low pressure pumps for large leaks and long-time cooling as well as high pressure pumps for small leaks.

Fig.8 shows the principle layout of the emergency core cooling system for a KWU-PWR. Aiming the reliability of this emergency core cooling system as high as possible, it contains 4 redundant, completely independent, parallel acting units. From Fig.8, in which the piping system and also the arrangement of the apparatus is somewhat simplified, one can see that 4 identical units can feed cooling water into the pressure vessel via the cold and the hot leg of each primary loop.

A more detailed and better up-to-date picture of one out of the 4 subsystems of the emergency core cooling system (ECCS) is shown in Fig.9. From this figure one can see that each subsystem has

1 high pressure pump,
2 accumulators and
1 low pressure pump.

The accumulators, which are filled with borated water at a pressure of approximately 30 bar, feed the coolant into the pressure vessels - even before the blowdown is finished - via self-acting valves. Calculations have shown that the action of these accumulators play a very important role for preventing unallowed temperatures in the core. The pumps get its borated cooling water during the first 30 minutes from a container. After this time enough primary coolant is collected at the bottom of the containment and the sucking pipes of the pumps are now switched over to this part, by which now the water before entering the pumps has to be cooled down in a heat exchanger.

This heat exchanger is connected through a cooling chain - which will be explained later in Fig.11 - to the river or another heat sink.

The layout of the complete emergency core cooling system is based on the very pessimistic assumption that one of the cooling units is not available due to inspection or repair work, another one fails, and that part of the water which is fed into the broken loop, escapes immediately out of the leak without reaching the core. The remaining amount of water hauled has to be sufficient to cool the core within the temperature limits given in the mentioned criteria.

3.2 The Emergency Feed Water System

After incidents or accidents which do not destroy the primary system and which do not lead to its depressurization, the emergency core cooling system described before cannot become effective. Also in case of a small leak, the energy transport out of the leak and the cold water supply by the high pressure pumps of the emergency core cooling system may not be sufficient to keep the core within safe temperatures. Therefore, another decay heat removal system has to be available. This is the so-called "feed water system".

In total the feed water system consists of 3 independent systems, each of which having a high redundancy, namely

- the main feed water system with 3 feed water pumps working in parallel,
- the start-up and shut-down feed water system, having 2 pumps also working in parallel, and
- the emergency feed water system, consisting of 4 completely independent units, each having its own Diesel-engine for driving via the electric generator-motor-mode a feed water pump.

The normal operating feed water pumps and also the start-up and shut-down pumps take its water from the feed water tank. Each of the 4 subunits of the emergency feed water system has its own storage tank where it can take the feed water from, in case the main feed water tank is not available. This emergency feed water system, however, can also be connected with the main feed water tank. The complete feed water system is shown in Fig.10. Figure 11 presents the emergency feed water system in more detail.

In case of a loss of all heat sinks but with pressurized primary system, pressure release valves being connected with the secondary side of the steam generators are opened and non-radioactive steam from this secondary side is blown to the atmosphere of the environment. Thus the steam generators are depressurized and a boiling occurs in the water of the secondary side. This boiling and steam generation acts as a new heat sink for removing heat out of the core, which is transported in the primary loops by free convection.

The water evaporated from the secondary side has to be replaced by the feed water system. For cooling down the reactor only two subunits of the emergency feed water system would be needed in an extreme case, and for just removing the decay heat one subunit is enough. The emergency feed water system has to be put in operation for example after an airplane crash, a chemical explosion, an earthquake or a station blackout, losing all electrical power.

The complete decay heat cooling device - in the form of one subunit of four - is shown in Fig.12. In addition to the unit of the emergency feed water system and the subunit of the emergency core cooling system, also the extra borating system for keeping the reactor subcritical is demonstrated in this figure. This figure also shows the complete emergency reactor heat removal string, which was mentioned before already, in chapter 3.1. This string transports the heat from the heat exchanger of the emergency core cooling system via a closed loop, equipped with two circulating pumps and a second heat exchanger, to the river.

This three-loop-system guarantees that no unallowable amount of radioactivity is transported to the river. Thanks to the high redundancy of all components in the emergency core cooling system and due to very careful repeated tests, the probability that the emergency core cooling system would fail completely is extremely small.

The fluiddynamic and thermodynamic conditions occurring during a loss-of-coolant-accident - with a large break or with a small leak, as well as those initiated by transients without a leak - will be explained in other lectures and its discussion is, therefore, omitted here.

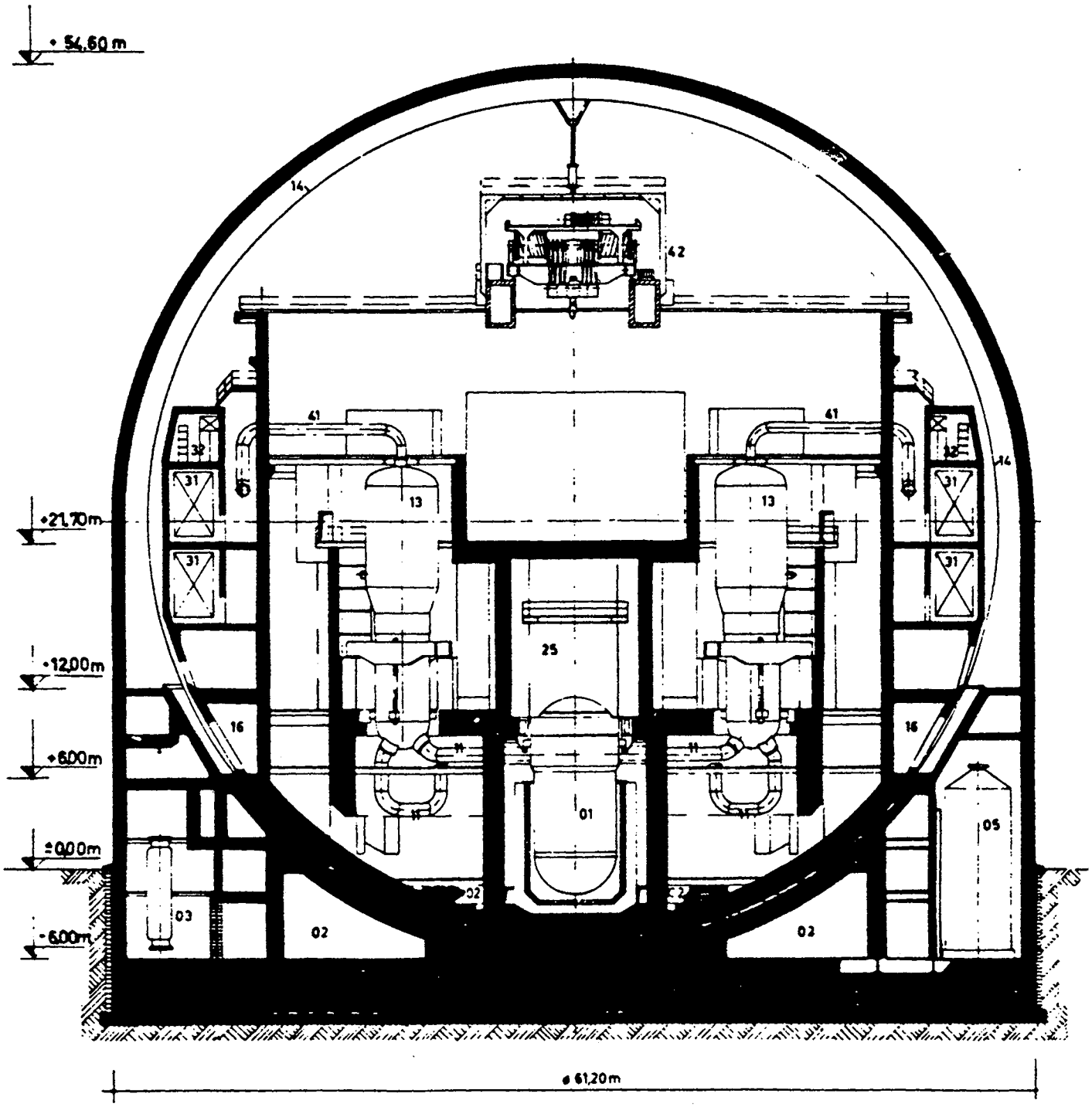


Fig. 1 : Primary System of a PWR

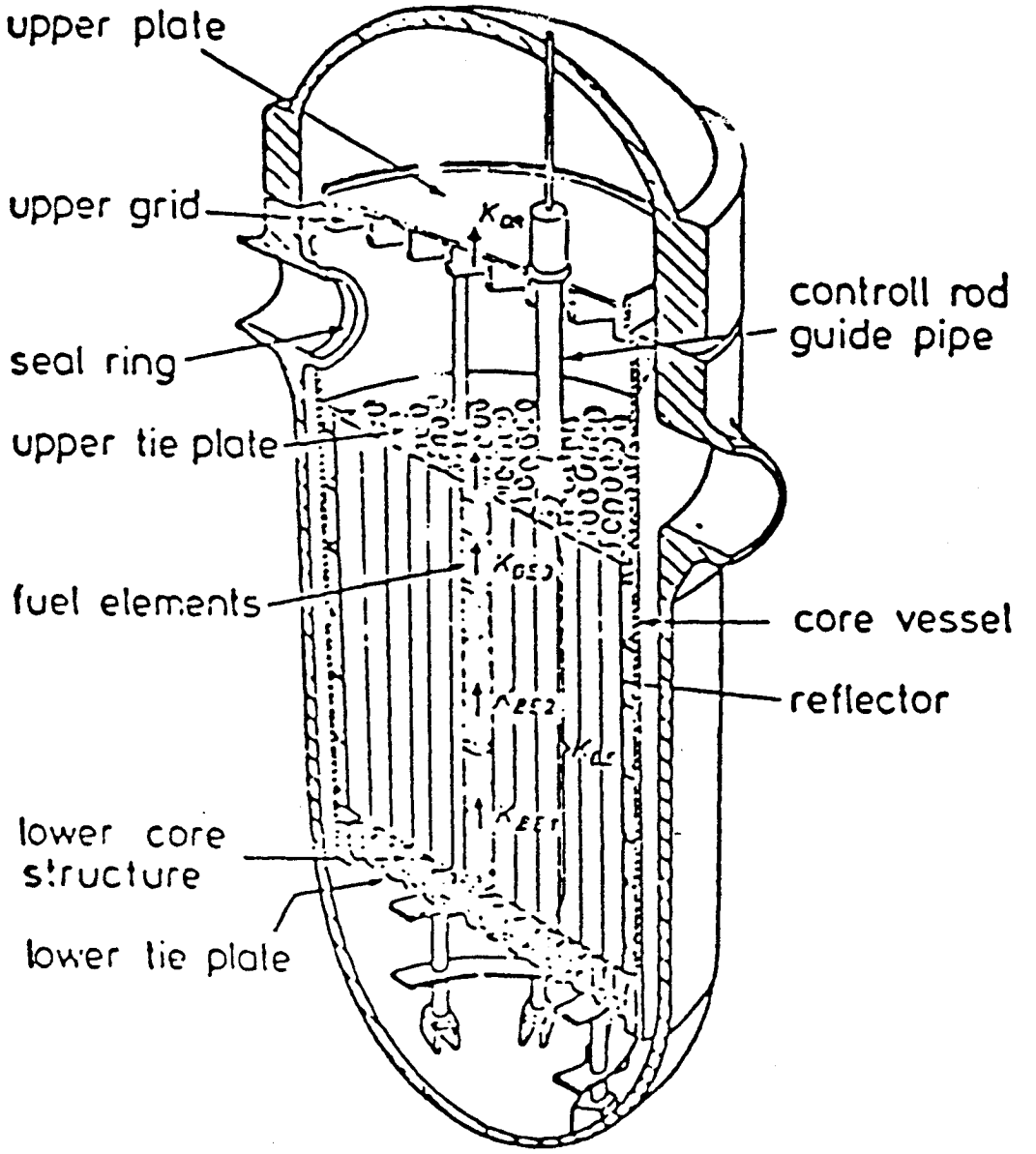


Fig. 2 : Pressure Vessel PWR

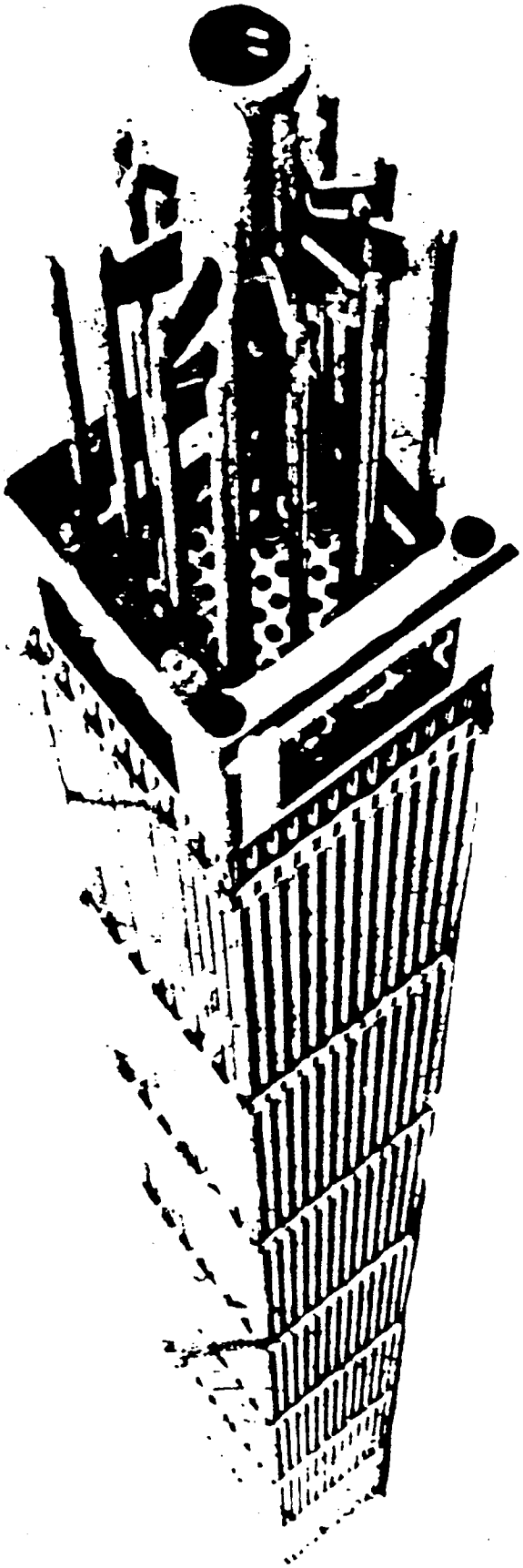


Fig. 3: Fuel Element PWR

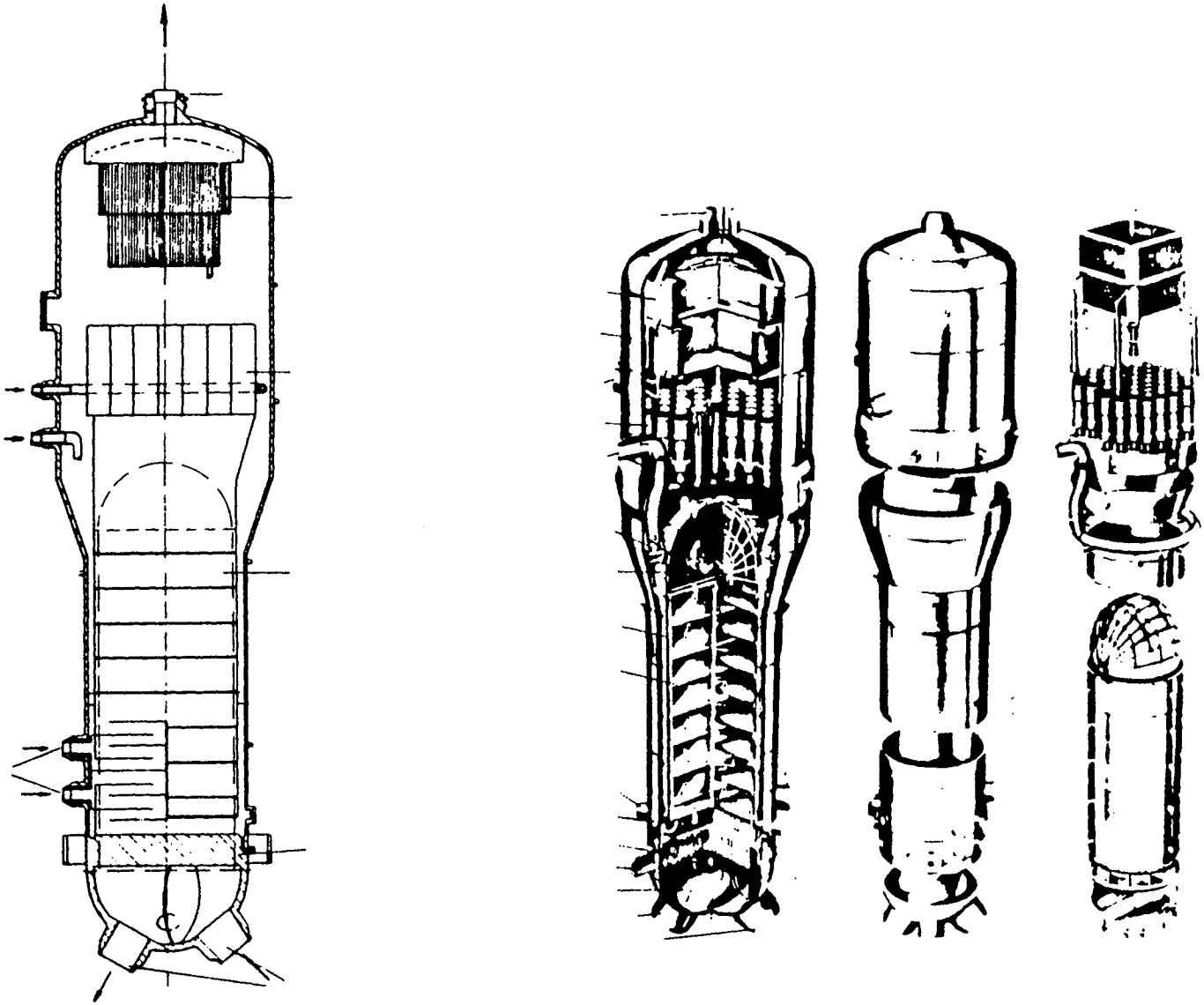
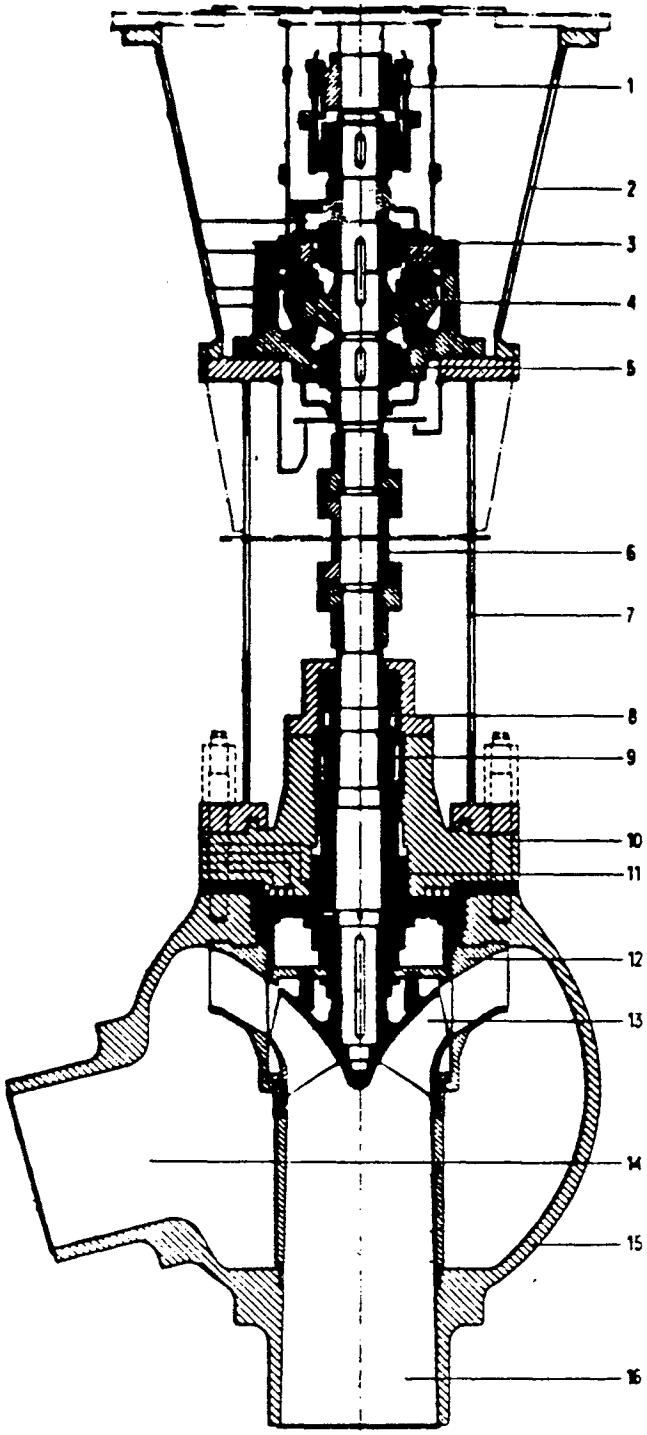


Fig. 4: Steam Generator PWR



Hauptkühlmittelpumpe.

1 Bogenzahnkupplung
2 Motorlaterne
3 Radiallager
4 Axiallager
5 Radiallager
6 Ausbaustück
7 Pumpenlaterne
8 ND-Wellendichtung
9 HD-Wellendichtung
10 Gehäuseflansch
11 Radiallager
12 Leitrad
13 Laufrad
14 Austrittsstutzen
15 Pumpengehäuse
16 Eintrittsstutzen

Fig. 5: Circulation Pump PWR

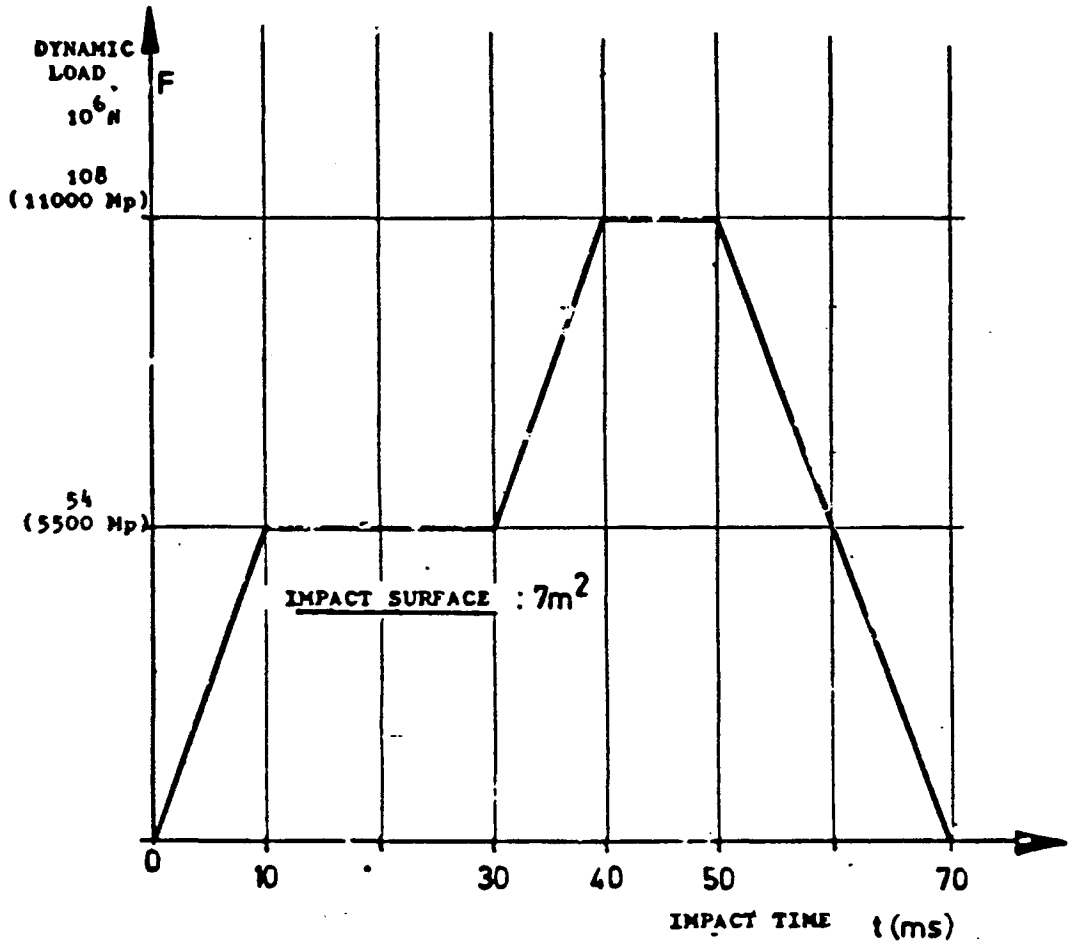


Fig. 6 : SHOCK - LOAD/TIME - DIAGRAM (AIRCRAFT UPON A RIGID WALL)

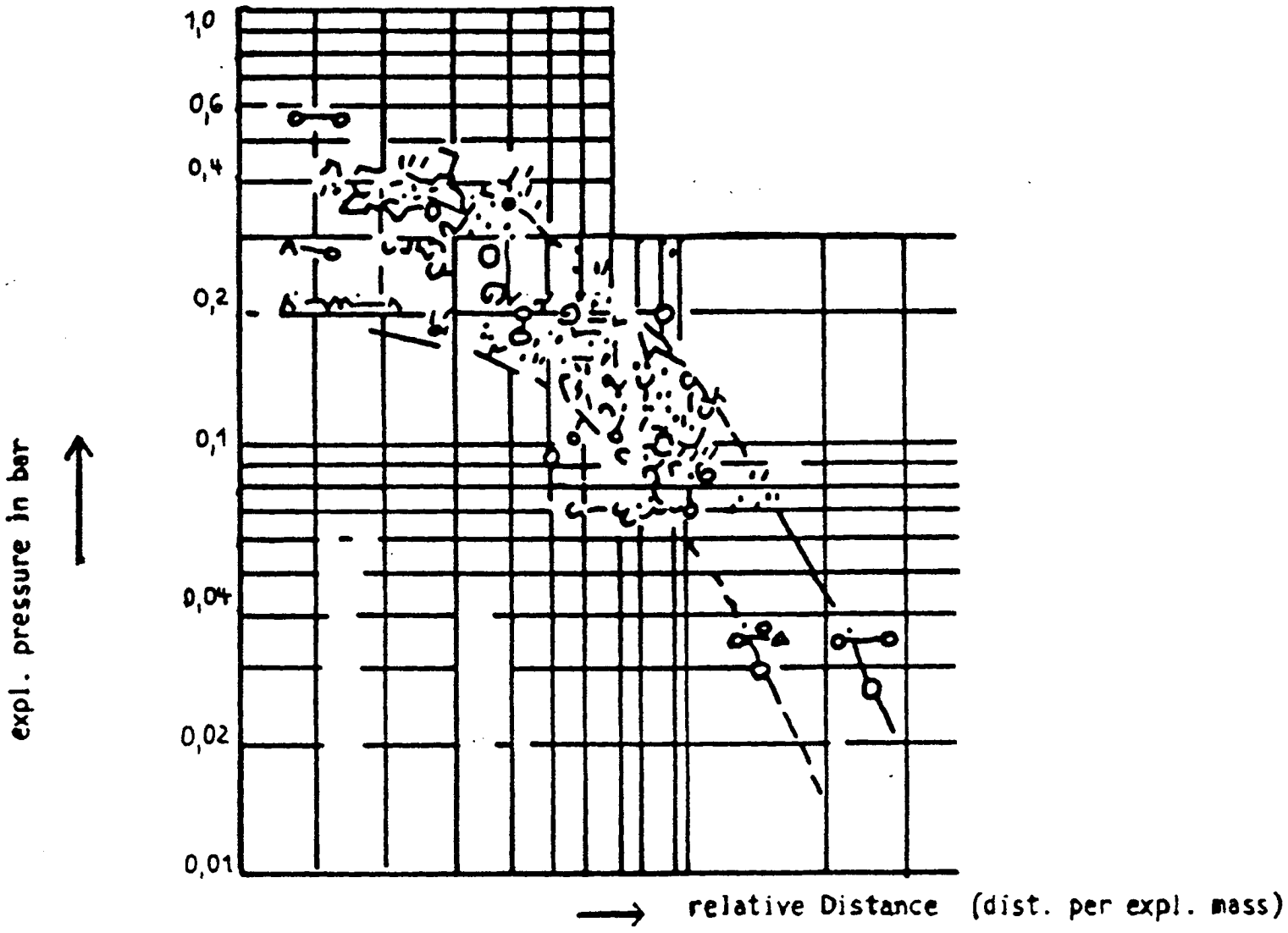


Fig. 7 : Pressures during Chemical Explosion as function of distance and exploded mass

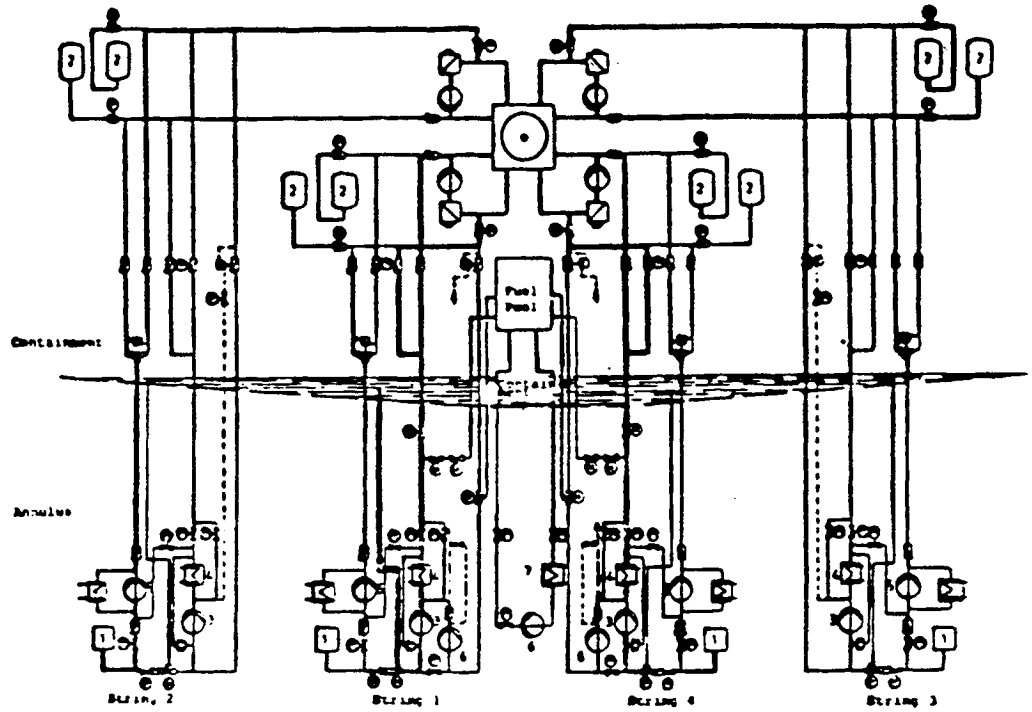
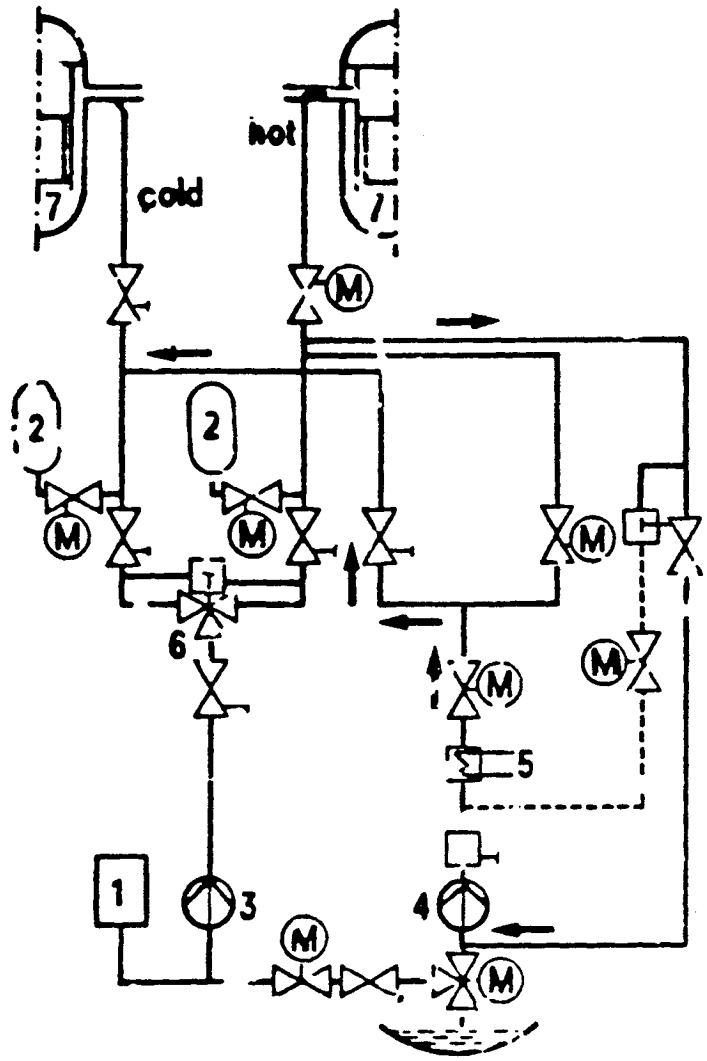


Fig. 8 : Emergency core cooling system



1 borated water storage tank
2 accumulator
3 high pressure injection pump
4 residual heat removal pump
5 residual heat exchanger
6 selection circuit
7 reactor pressure vessel

KWU–ECCS (1 of 4 Subsystems)

Fig. 9 :

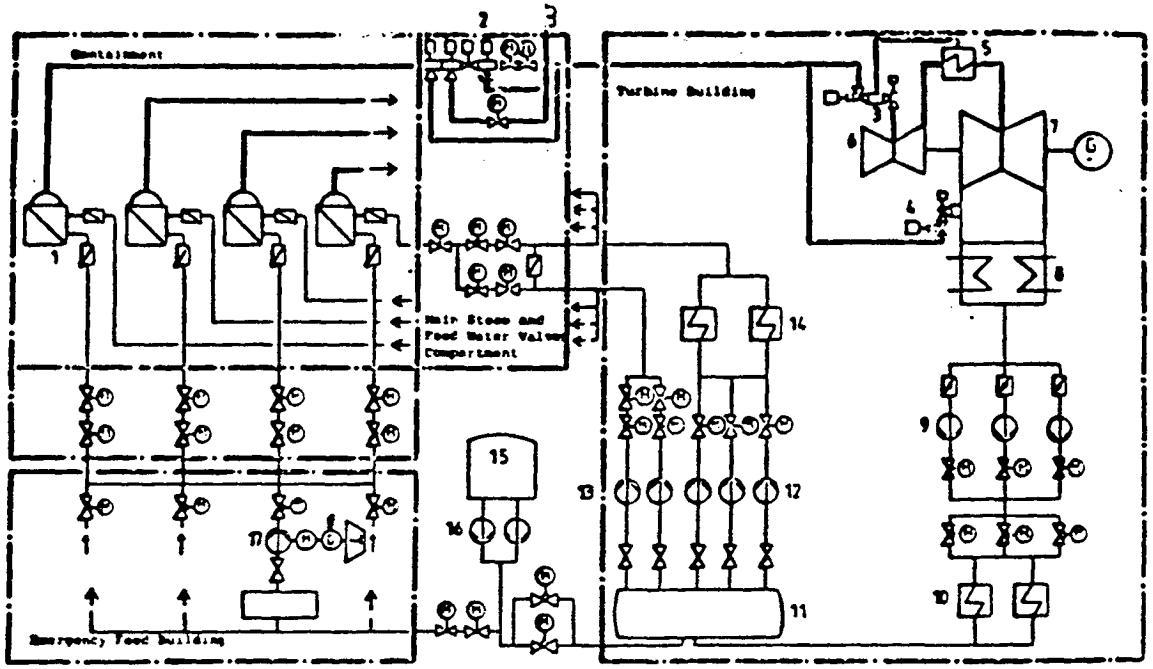


Fig. 10 : Feed water system

1 Steam Generators
2 Main Steam Valves
3 Quick Closing Valves
4 Bypass Valves
5 Reheater
6 HP-Turbine
7 LP-Turbine
8 Condenser
9 Main Condensate Pumps
10 LP-Feedwater Heaters
11 Feedwater Tank
12 Main Feedwater Pumps
13 Start-up and Shut Down Pumps
14 HP-Feedwater Heaters
15 Demineralized Storage Tanks
16 Demineralized Water Pumps
17 Emergency Feedwater Pumps

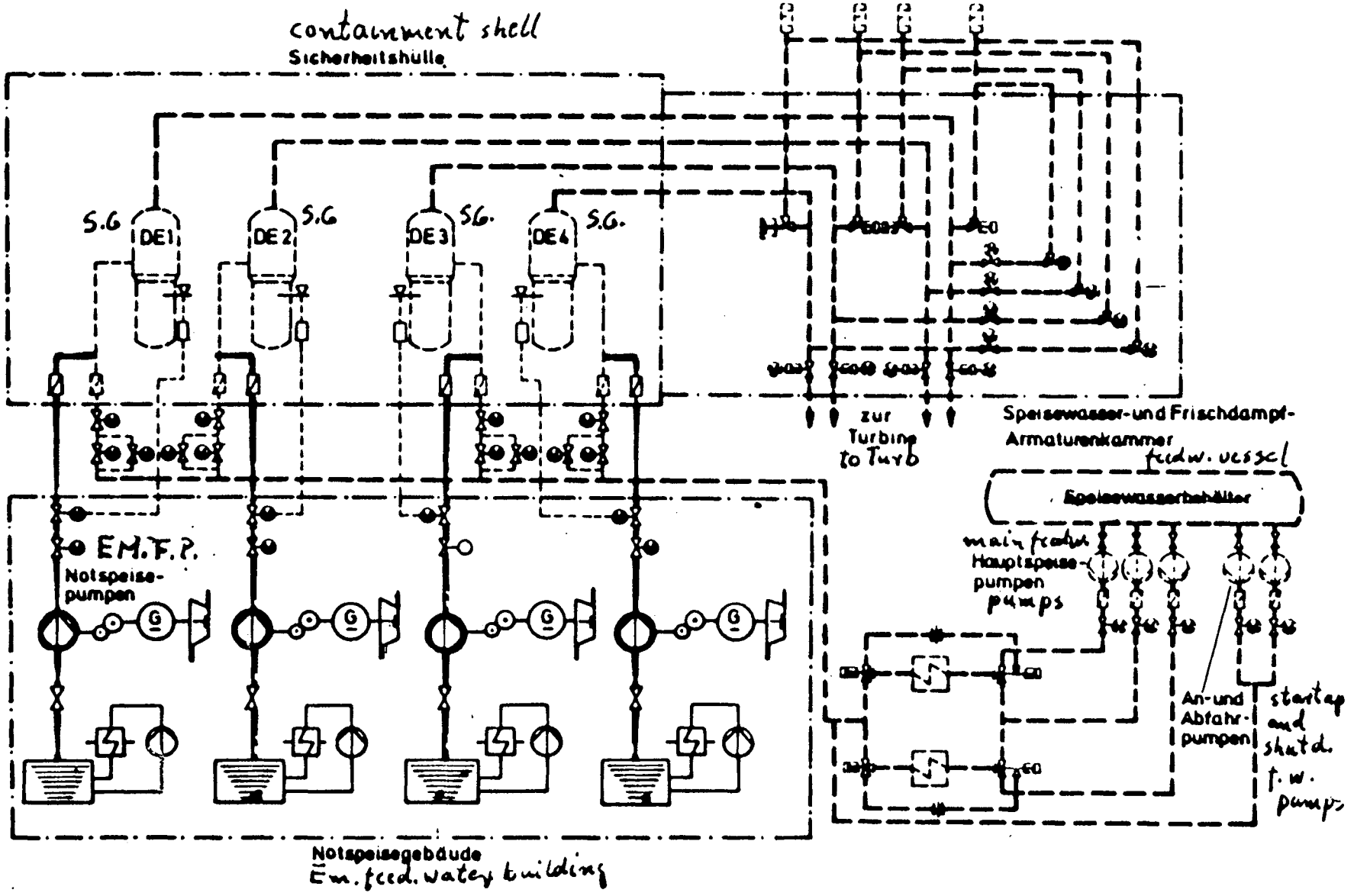


Fig. 11 : Emergency feedwater system of a 1300 Mwe plant

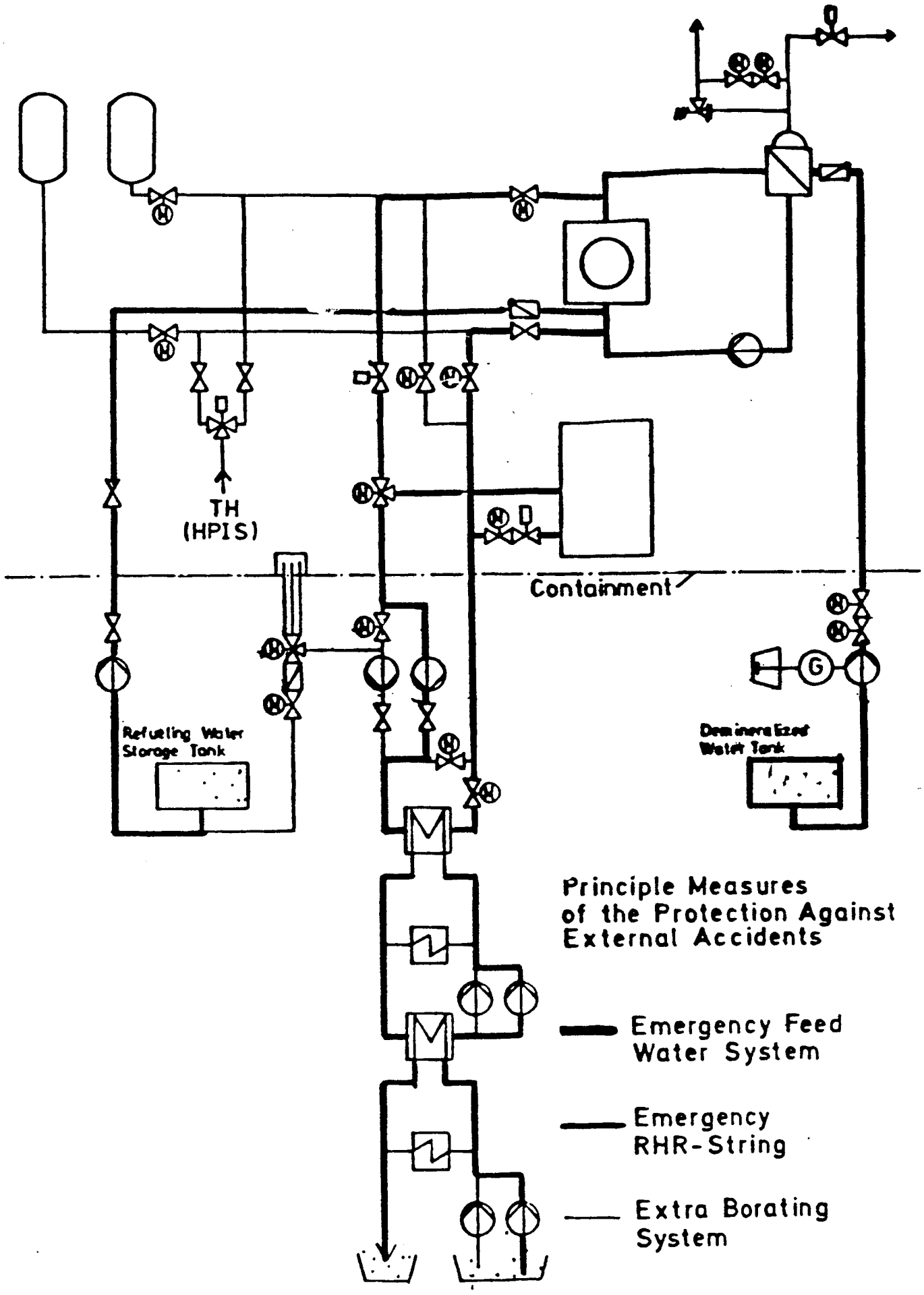


Fig. 12 : One complete string of decay heat removal system

I S P R A C O U R S E

Thermohydraulic Problems Related to PWR Safety

Introduction to PWR Safety

PART II: Severe Accidents

by F. Mayinger

---

1. Classification of Accidents

In the past licensing of nuclear power plants was mainly concerned with a break of a large pipe in the primary system. The so-called "design basis accident" was defined, which would be the total break of one of the main coolant lines in the primary system. For large nuclear power stations of approximately 1300 MW_e these lines have a diameter of 700 to 800 mm. From risk studies and, last not least, from the Three-Miles-Island reactor at Harrisburg we know that small leaks and transients without leaks - for example a station blackout - have much higher probabilities (Fig.1).

Beyond the "design basis accident" one can distinguish three categories of hypothetical accidents, as classified in Fig.2. The accidents belonging to the first category can be mastered by the safeguard- and emergency core cooling systems without any additional measures, and with the cladding of the fuel elements remaining within the temperature limit of 1200°C, as stated in the international guidelines. Here we have to recall the fact that licensing analysis up to now is usually performed by conservative assumptions. Doing a best-estimate analysis, one realizes that the maximum cladding temperatures are predicted much lower than under conservative aspects (Figs.3 and 4). The main difference between conservative and best-estimate presiction is coming from the assumption in the licensing analyses that one of the four emergency core cooling strings fails when it is called for operation, one is under inspection or repair when the accident occurs and, finally, a third one feeds partially to the leak only.

Thus the capacity of only one and a half emergency core cooling strings are active and available for temperature reduction of the fuel elements and for decay heat removal (Fig.3).

As mentioned, in case of a small leak the heat from the core is removed via free convection to the steam generators, and by blowing down the secondary side of the steam generators. There is no danger of core damage at all, as long as the water level or - at least - the mixture level stands above the upper fuel element end-boxes. This water level is guaranteed as long as, at least, two safety injection pumps feed into the primary system and the secondary side of, at least, two steam generators is cooled down with 100 K/h.

A "Category II"-situation would mean that the emergency core cooling systems would fail for a certain period of time which has the consequences of severe core damage, but by reinforced cooling, however, a long-term decay heat removal can be reached and the core can be cooled down again. As discussed later, the TMI-accident fits within Category II.

Category III-accidents are sequences with complete core melting and penetration of molten corium into the containment. This presumes that all emergency core cooling systems fail completely and for a very long time.

2. Accidents of Category I

With large leaks and a slightly detoriated emergency core cooling system, temperatures in the order of 800 to 1000°C of the cladding material in the core can occur. This would mean that the cladding would be ballooned by the high pressure inside the fuel rods, which originates from the fission gases. This ballooning creates a partial blockage of the cooling flow channels in the fuel element, however, measurements (Fig.5) showed that this blockage is

not reducing the heat transfer from the fuel rods and, by this, is not increasing the temperature of the cladding. With higher temperature the cladding may burst, however, this would even improve the coolability of the fuel pellets.

With small breaks or small leaks the high-pressure injection system can overcome the loss of coolant in most cases. Fig.6 shows that two high-pressure safety injection pumps are enough to keep the water level in the pressure vessel of the primary system above the upper end of the active core length. This means that no core damage would result in such a situation, however, the primary system would not be completely filled with liquid water. Thus, a single-phase liquid natural convection between the core and the steam generators cannot be sustained. Therefore, a two-phase flow convection, and in some parts of the primary system a single-phase vapour flow convection, takes over the task of cooling. Steam evaporated in the core flows through the hot leg to the steam generator, is condensed there and returns in the form of liquid water, either through the cold leg or in a countercurrent flow through the hot leg to the pressure vessel of the primary system and, by this, to the core. This so-called "boiler-condenser-mode" of cooling works even if non-condensable gases are in the primary system. These non-condensable gases can be fission-gases from bursted fuel rods, or nitrogen which originated from the accumulators, because high-pressure nitrogen is used there to press the water into the primary system in case of a loss-of-coolant accident.

The behaviour of the non-condensable gas in the steam generator is shown in Fig.7. One can see that the non-condensable gas is mainly concentrated in the down-facing part of the U-tubes of the steam generator. The vapour condenses in the up-facing part of the steam generator and the water flows back via the hot leg to the core. The temperature difference between the two-phase mixture in the core and the fluid in the steam generator, needed

for driving the free convection in case of the boiler-condenser-mode, is even smaller than in the case of liquid single-phase natural convection. As Fig.8 shows, it increases with adding non-condensable gas to the two-phase flow mixture, however, it still remains within limits which guarantee a safe cooling of the fuel elements in the core. So Category I-accidents, even with a partially empty primary system, would not result in a core damage.

3. Accidents of Category II

Each hypothetical accident starts from a situation where from a certain period conditions of Category I exist. The duration of this period is increasing with decreasing leak size, as Fig.9 demonstrates. With small leaks there is one hour time of tolerance, and with no-leak-transients there are more than two hours time of tolerance until failed emergency systems have to be reactivated or additional measures have to be taken. This reinforcement or reactivation of safety systems has to be done by the operator. For a proper and correct action of the operator in case of a hypothetical accident, two conditions have to be fulfilled:

- The operator must get correct and reliable informations about the situation in the pressure vessel, and
- the operator must have a clear idea what would be the best measure to master the accident.

To fulfill the first condition a further improvement of the instrumentation, giving information about the cooling conditions in the core, would be desirable. Therefore, an in-core water-level measuring device was developed in the Federal Republic of Germany and is presently tested in a commercial nuclear power plant.

For matching the second condition the operator needs an excellent training in which he learns to overcome situations of hypothetical accidents, too.

In Fig.10 the tolerable activation delay of heat removal systems for large-break situations is tabulated. The first row of this table demonstrates that only one low-pressure heat removal pump is needed to keep the maximum cladding temperature below 1200°C, even if assuming that none of the 8 accumulators will be available, which seems physically impossible. With 7 accumulators becoming active after depressurization, there is a tolerance of approximately half an hour until one of the low-pressure pumps must feed water into the core to avoid that the core temperature exceeds a value which would mean that core melting starts. This is assumed to be approximately 1900°C. With small leaks the situation is a little more complex. Here we have to ask, what time is needed until the safeguard system detects the leak. There are three different signals announcing a leak, as demonstrated in Fig.11. Due to easily understandable physical reasons the response-time of these signals is a function of the leak size, as also shown in Fig.11. Looking at this figure we have to realize that for very small leakage sizes - smaller than 1,5 cm^2 - no emergency core cooling system is needed because the volume controlling system feeds enough water into the pressure vessel to keep up the water level high enough. So in any case the high-pressure injection pumps will be activated early enough. There is plenty of time for activating the secondary side blowdown, even if only one high-pressure safety injection pump would be available.

As shown in Fig.12, this tolerable delay of secondary side blowdown activation goes up to 3 hours for one safety injection pump and reaches 5 hours with two safety injection pumps for small leaks. Staying within this time of tolerance would mean that the temperature in the core would not exceed 1200°C. This time of tolerance becomes much larger before a situation in the core or in the primary system develops, which would go beyond the consequences of Category II-accidents. Also in a Category II-situation the operator has several possibilities to act in a proper way.

4. Category II-situations during the TMI-accident

The Three-Miles-Island accident (TMI-accident) which occurred in March 1979 was, in the meantime, a subject of several safety analyses. A most recent analysis was given by the National Research Center at Idaho. Calculations were performed there, based on three different assumptions, for the time course of the water inventory in the primary pressure vessel. These assumptions were

- a late uncovery of the core,
- an early uncovery of the core, and
- an uncovery with zero make-up.

The time history of the two-phase liquid level in the core for these three assumptions is shown in Fig.13. One can see that the core was twice almost completely uncoverd; the first time approximately 175 min and the second time approximately 205 min after the accident started (Fig.13). The uncovery with the assumption of zero make-up is unrealistic and, therefore, will not be discussed here. The temperature of the cladding must correspond to the uncovery history of the core. That this is the case demonstrates Fig.14. As mentioned, the timely course of the mixture level and of the cladding temperature - shown in the Figures 13 and 14 - is a result of theoretical analyses, based on post-examinations of the core damage. During the accident, however, the pressure was measured and the timely course of this pressure measurement is given in Fig.15.

From these analyses one can draw the conclusion that the core damage in the reactor made progress in three time-steps:

- In the period between 100 and 174 minutes after the accident started, a heating up in the pressure vessel occurred and the core started to become dry, as a consequence of the loss of coolant.

- In the period between 174 and 229 minutes after the accident started, the core was further heated up, due to insufficient water injection by the emergency core cooling pump in one of the loops. During this period a brittle failure of the fuel rods took place in the upper part of the core and an empty space was formed there.
- Beginning with the 227th minute after the accident started, molten core material was moving downward into the lower part of the core, but the emergency core cooling water now transported into the core could stop the melting and reduce the temperature again.

The core conditions during this period of core melting - 174 and 225 minutes after the accident started - as the above mentioned analysis predicts, are demonstrated in the Figures 16 - 18. One can see from these figures that at first in the lower half of the core a relocated and partially solidified prior molten core material occurred, which was followed after a few minutes by a debris bed of oxidized and previously molten fuel rod material in the upper part of the core. Finally, after approximately 200 minutes, the lower support plate of the core was destroyed and a prior molten debris fell into the lower plenum of the pressure vessel. This debris consisted of small particles of coolable size and geometry. The pressure vessel was not affected by the melt.

A summary of the damage is represented in Fig.19. Important readings from there are that peak temperatures of 2900-3100 K were reached in the upper part of the core, and that a significant fuel liquefaction and fuel melting with subsequent relocation took place. The estimated fuel inventory in the lower plenum after the accident may be as high as 20%. The most important conclusion from this analysis, as listed in Fig.20, is that the progression of the accident was terminated, when the high-pressure injection pump was started again after approximately 200 minutes and, by this, enough cooling water entered the pressure vessel again. This means, during a hypothetical accident one should

take any effort to bring water into the pressure vessel, independent of the accident scenario. The pressure vessel wall will not be seriously affected by a partial core melting.

5. Consequences of a Category III-accident

A Category III-accident can only develop if all emergency- and decay heat removal systems fail for a long time, or cannot be reactivated within a certain period. Assuming this total and permanent failure of all decay heat removal systems, a core melt accident would develop with a time history as shown in Fig.21. There is only a small difference in time until the melt would come in contact with the water in the sump for a large break (low-pressure case) and for a small break or a no-leakage transient (high-pressure case). Theoretically, there are four paths how the integrity of the containment could be violated and how, by this, radioactive material could escape into the environment to a not permissible extent:

- steam explosion
- penetration of the core foundation
- hydrogen explosion or detonation
- overpressurization

There were long discussions whether a steam explosion - which is a thermal interaction between liquid molten corium and water - can destroy the containment or even the pressure vessel. Two situations are imaginable in which an explosive-like interaction between molten corium and water could occur.

In case of a large leak a steam explosion could be ignited during the period when the melt flows from the core region into the water being still present in the lower plenum. In case of a small leak or a station blackout, this situation of flowing melt into the water of the lower plenum would need an extremely high triggering energy. During the TMI-accident molten core was flowing into the water pool of the lower plenum, however, no steam explosion was observed. After having penetrated the pressure vessel

the corium melt could again come in contact with water, when the concrete shield around the pressure vessel fails, due to the thermal attack by the melt. Here, however, the mixing energy between melt and water is very small because water will slowly flow over the molten pool or melt will creep under the water and, therefore, almost no mixing occurs. This condition will not lead to a powerful steam explosion. Here one has to mention that the design of the cavity under the pressure vessel in German pressurized water reactors is different from US-types - as shown in Fig.22 - because there is a dry cavity under the pressure vessel.

In view of the very difficult situations with clarifying the physical phenomena during steam explosions, a research project was started in the Federal Republic of Germany, which attacks the problem from the mechanical side. The question was rised, how much melt has to react within a few milliseconds to destroy the pressure vessel and, in consequence, the containment. This theoretical analysis was based on all available data to be found in the literature. It finally came out that under worst conditions and most possimistic assumptions the pressure vessel of a German 1300 MW_e-design could withstand a steam explosion, where 50000 kg corium are interacting instantaneously with water and being premixed and prefragmented in particles of a few millimeters diameter at a volume ratio between water and melt of 1:1, which would be the most pessimistic volumetric condition. It is physically impossible that such a large amount of melt is premixed during a core-melt-down accident within these conditions and without a small steam explosion being triggered, before this premixing of that large amount is completed.

As a consequence of these deliberations, a steam explosion which would destroy the pressure vessel or the containment must not be taken in account in risk deliberations.

As Fig.23 shows, the minimum mass of molten corium reacting with water would be much higher than 50000 kg, if physically more realistic assumptions are supposed in the calculation. A fragmentation of melt down to homogeneous particles of only 15 µm diameter - as assumed in the case of 50000 kg - seems to be physically impossible.

The concrete foundation of German pressurized water reactors is very strong, because it has to carry the concrete dome around the containment sphere which protects the containment against missiles from outside after an airplane crash-down. Calculations based on experiments showed that it would take several days until the melt could penetrate this concrete foundation, and the melt would freeze latest in the soil below the concrete forming a rigid shell of condensed solid material arount it, which was produced by the heat attack of the freezing melt. The radiological impact onto the air of the environment would be small along this path.

Hydrogen deflagrations, in case of a core melt accident, are very likely. They also occurred during the TMI-accident. Experiences from experimental and analytical research allow to draw the conclusion that the maximum pressure peak resulting from such a deflagration will be lower than the design pressure of the containment. Such deflagrations can occur within the first hours up to the end of the first day after the accident started. Assuming a homogeneous mixture of hydrogen, air and vapour in the containment and in its various subcompartments, the hydrogen concentration would stay outside the detonation region for the high-pressure case as well as for the low-pressure case, as shown in Fig.24. With nonhomogeneous mixing - which is more probable than the homogeneous one - concentrations in one or the other subcompartment may occur, which are near to or even within the detonation limits.

The detonation limits shown in Fig.24, however, are for hydrogen-air-steam mixtures and neglect the influence of water droplets, which are certainly present in the containment during this accident. The damping effect of the droplets can retard a detonation remarkably.

Mainly due to evaporation of water - but to a small extent also by carbondioxide formation - the pressure in the containment starts to rise approximately 10 hours after the accident happened. The produced CO_2 (also H_2,CO) originates from the melt-concrete interaction and the evaporation is a consequence of the contact between melt and sump water. Fig.25 shows the containment pressure history as it was calculated for the low-pressure case, that is, after a double-ended break. One can see from this figure that the partial pressure of H_2O plays the dominant role in the containment pressure-time history. After a period of 4 to 5 days the pressure in the containment would reach the failure limit.

This pressure-time history is only slightly different in the high-pressure case, as shown in Fig.26. The pressure peak around three hours after the accident started is a little more pronounced than in the low-pressure case, which results from the fact that in the moment of the reactor pressure vessel failure the accumulators inject its water into the melt. In the low-pressure case this accumulator injection happens before the core starts melting. This pressure peak - resulting from this accumulator injection - in the high-pressure case, however, stays below the design pressure of the containment, as Fig.26 demonstrates.

In the meantime a plant-specific analysis showed that overpressurization would not cause in any case a catastrophic failure of the containment but, at first, could have the consequence that some penetrations for pipes or instrumentation lines or also flanges would not start to leak. As soon as the volumetric flowrate through these leaks is equivalent to the vapour-volume produced by evaporation, the pressure in the containment would remain constant.

6. Licensing principles

The expression "severe accidents" is used for those events, which progress beyond the design basis of a nuclear power plant and, eventually, result in a degradation of the core. Licensing with respect ot these severe accidents should agree on two fundamental points:

- The prevention of accidents has priority over mitigation of accident sequences and
- whether and which additional safety systems are advisable to minimize technical risks has to be decided on the basis of sound analyses of the real system behaviour in case on an accident.

In the Federal Republic of Germany - due to very stringent requirements to protect nuclear plants against external impacts - - vital system functions like emergency power- amd emergency feed water supply are installed with extremely high redundancy. The issue of severe accidents has not been addressed in terms of quantitative frequences and consequences, however, priority is given to the analysis and - if advisable - to the improvement of the potential of existing systems to maintain sufficient core cooling, even under adverse circumstances.

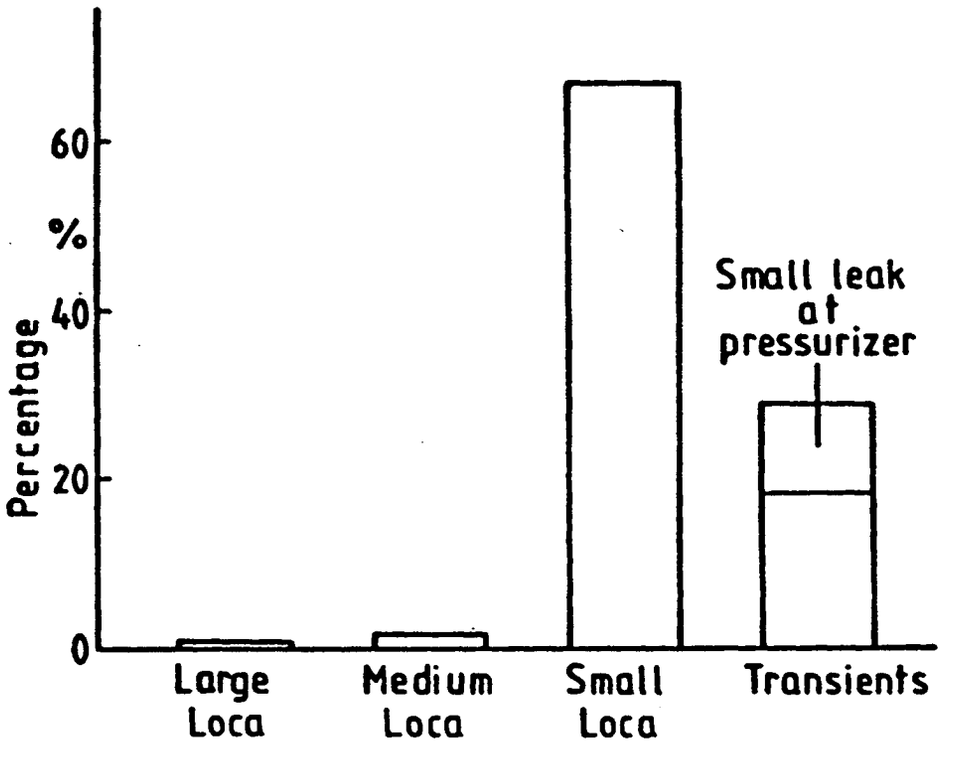


Fig.1 : RESULTS OF EVENT TREE ANALYSES

CATEGORY	I :	Requirements of licensing not fulfilled, but full coolability of the core possible with remaining safety systems. Temperature limits of licensing not exceeded.
CATEGORY	II :	Accident sequences with severe core damage. By reinforced cooling, however, a long-term decay heat removal can be reached. (TMI acc.)
CATEGORY	III :	Accident sequences with complete core melting and penetration of molten corium into the containment.

Fig.2 : Classification of accidents

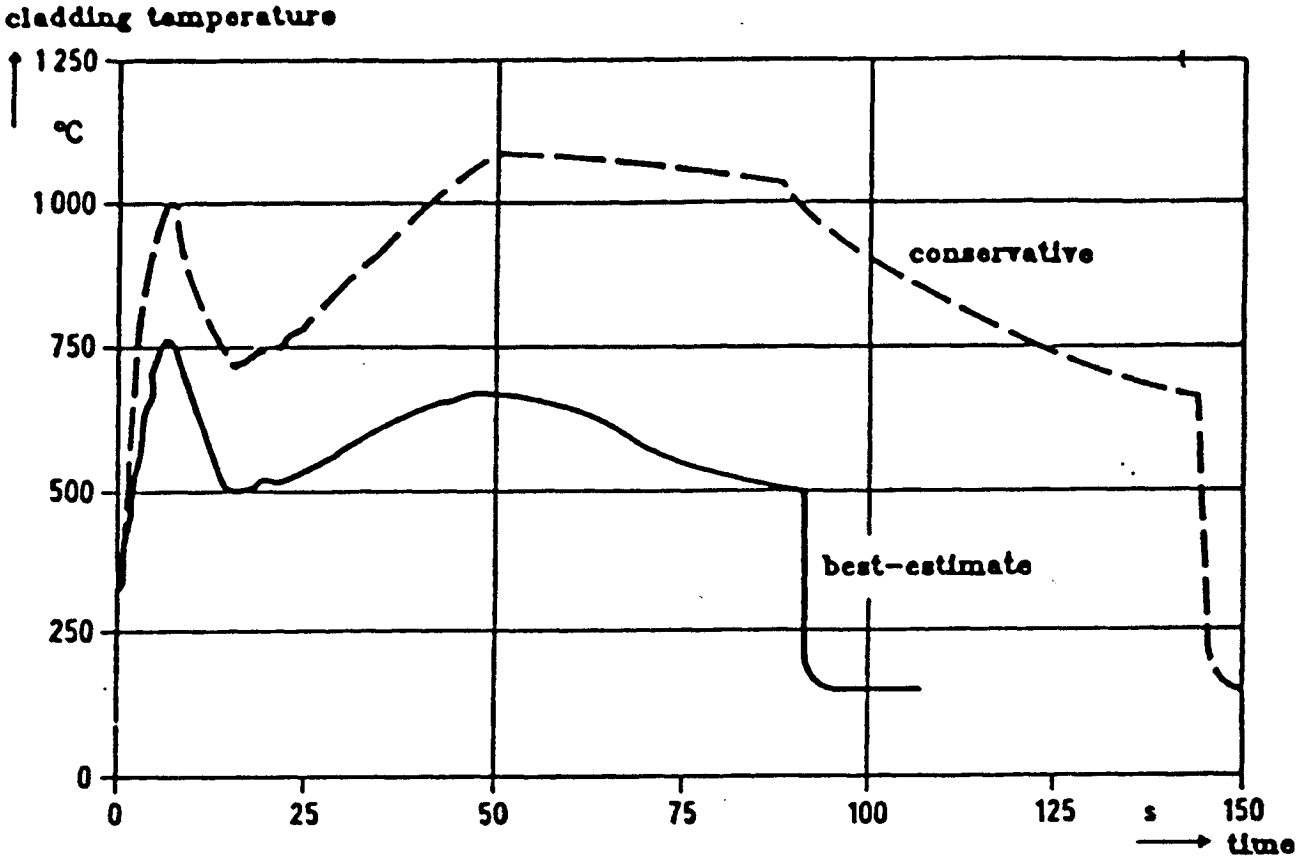


Fig.3 : Cladding temperatures for a hot rod, 1300 MW, PWR, 2 F-break between pump and pressure vessel

	licensing procedure	"best-estimate"
Initial Power	1o6 %	1oo %
Discharge Model	Moody	homogen-isentrop
Decay Heat	1.2 * ANS	1.o * ANS
Condensation Efficiency	o.6	o.8
State of Main Coolant Pumps during Refill and Reflood Phase	blocked	unblocked
Power Factor	2.5	2.o
Flow Reduction Factor in Hot Channel during Blowdown	8o %	1oo %
Single Failure and Repair Criterion	yes	no

Fig.4 : Main assumptions for "best-estimate" and conservative blowdown-and reflood-calculations

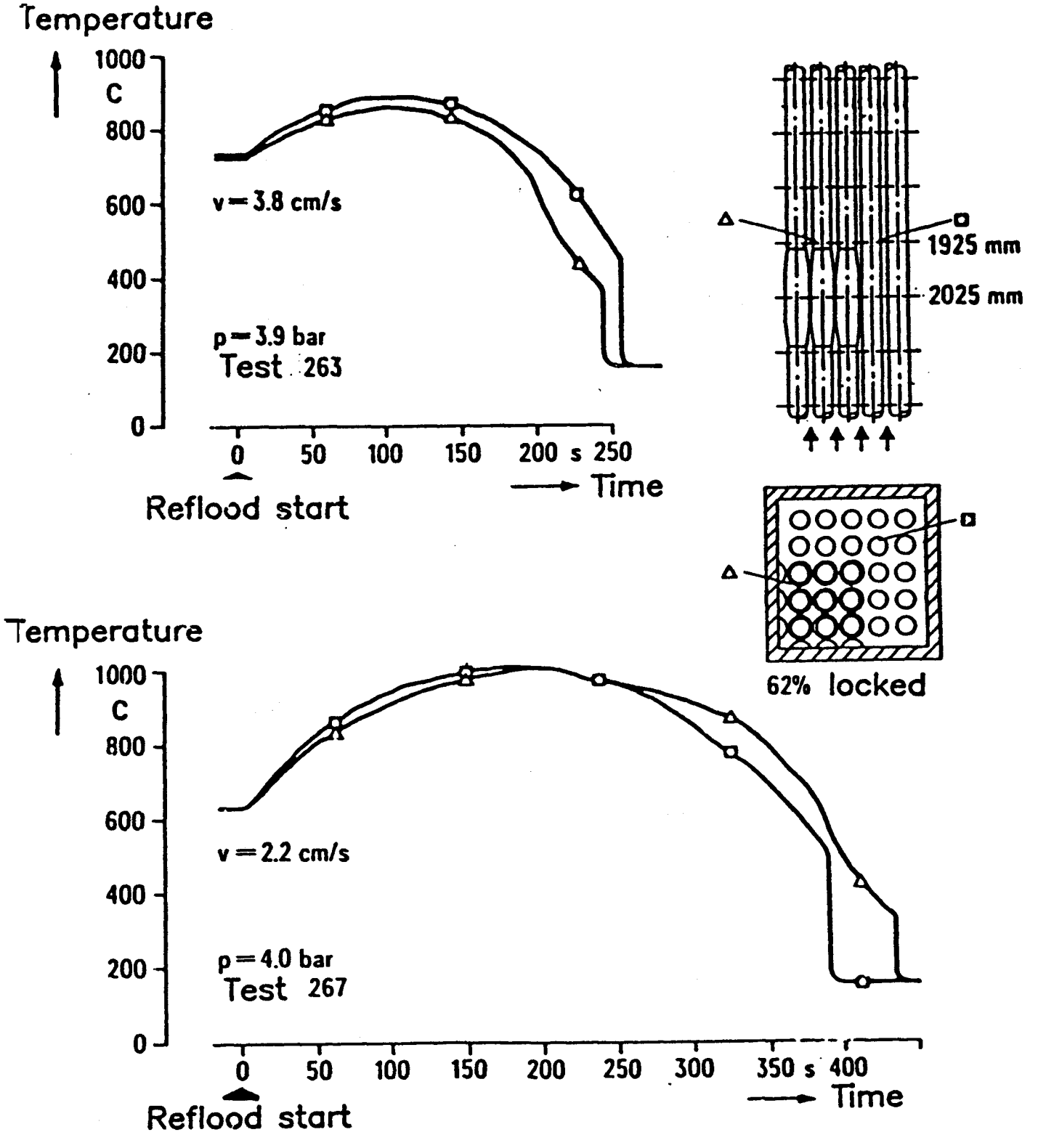


Fig.5 : **Reflood test: Temperature of cladding in a partially locked bundle**

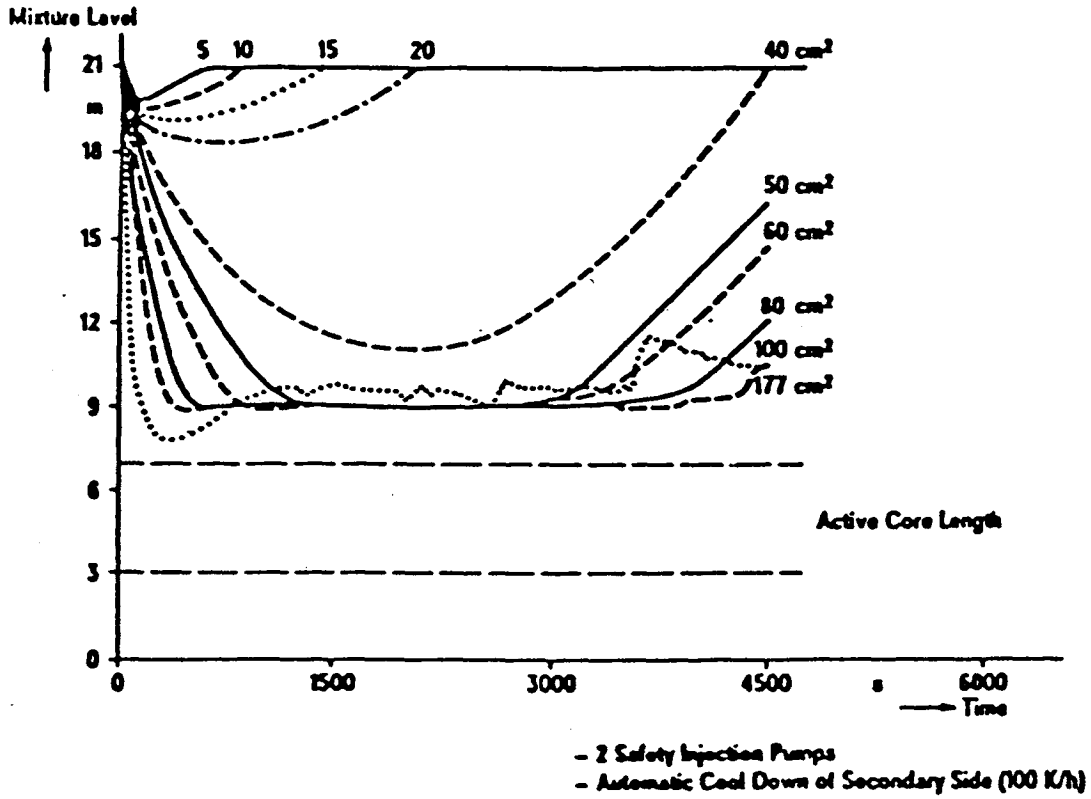


Fig.6 : Behaviour of water level with small leaks

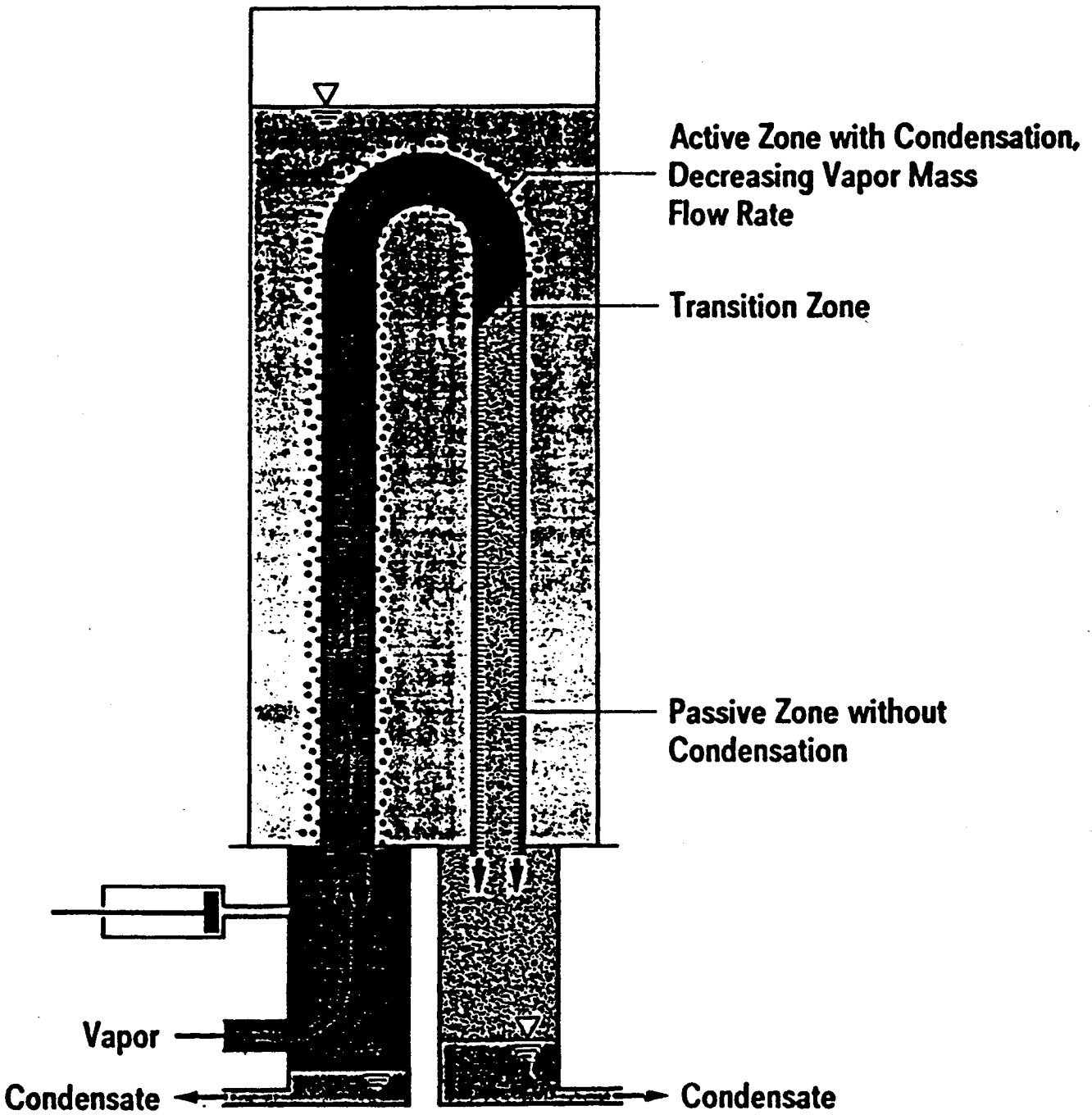


Fig. 7 : Behaviour of Non-Condensible Gas in Steam Generator

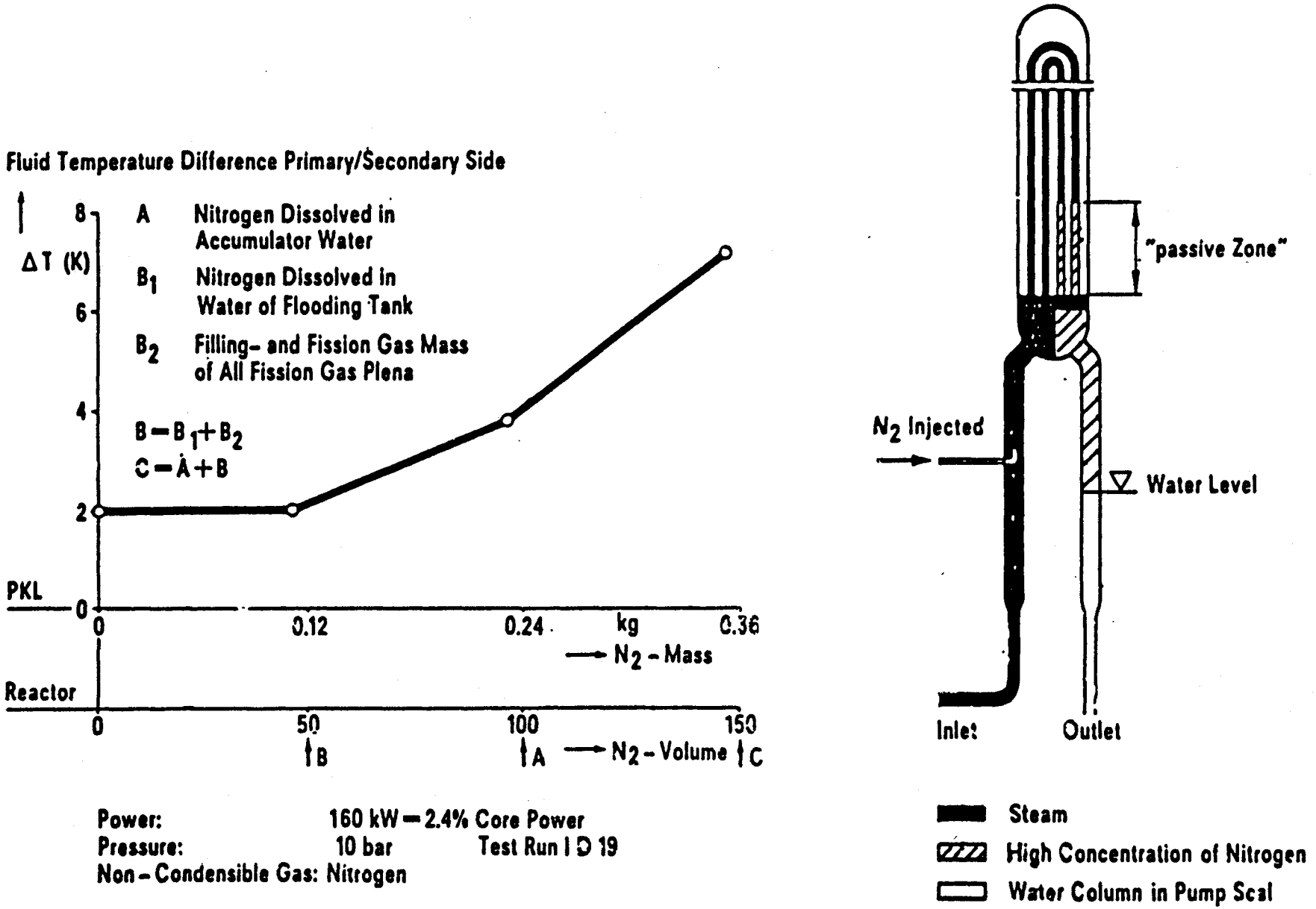


Fig. 8 : Driving temperature difference for the boiler-condenser mode

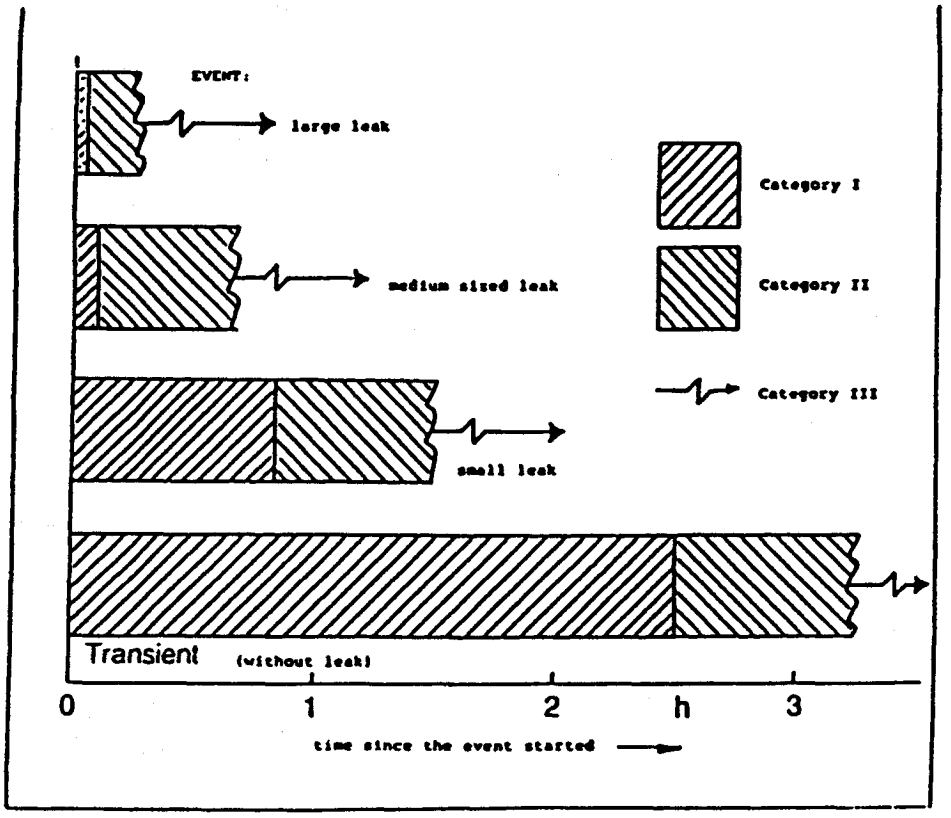


Fig.9 : Time history of hypothetical accidents and time of tolerance for reinforcing safety systems

LARGE BREAK

break size	location	availability of systems SIP	Accum.	RHR-pump	activation delay of RHR-pumps
2.A	cold leg	0 of 4	0 of 8	1 of 4	none
2.A	cold leg	0 of 4	7 of 8	1 of 4	0.5 h

Fig.10 : Tolerable activation delay of residual heat removal (RHR) pumps to avoid local core melting

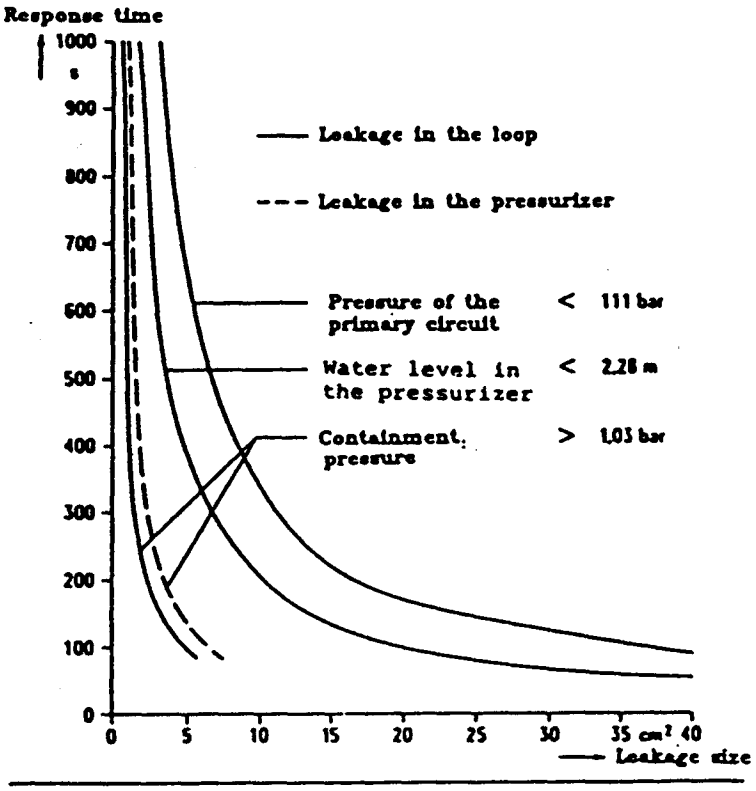


Fig.11 : Response time of safety signals of a 1300 MW PWR

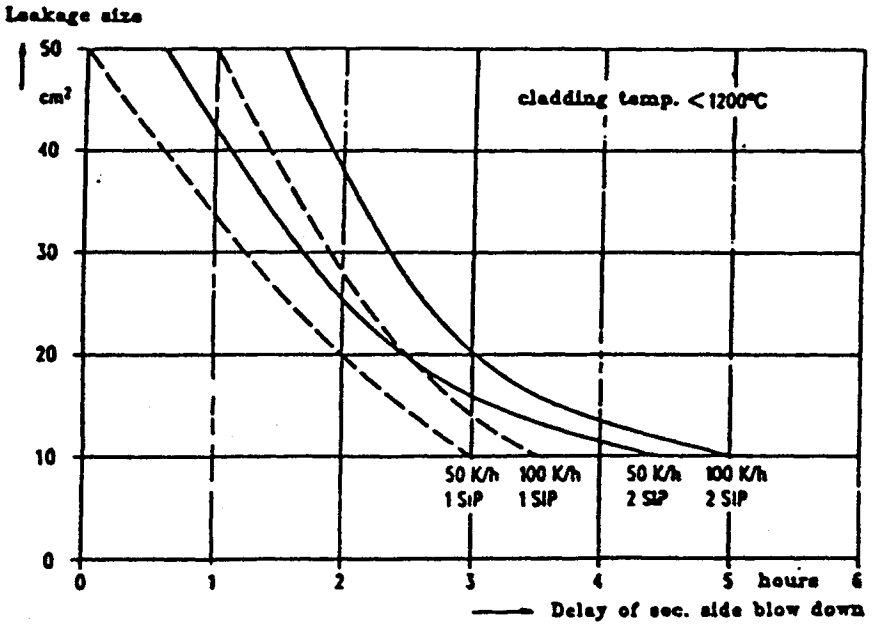


Fig.12 : Emergency cooling analysis in case of reduced system availability and delayed sec.side blow-down (1300 MW PWR)

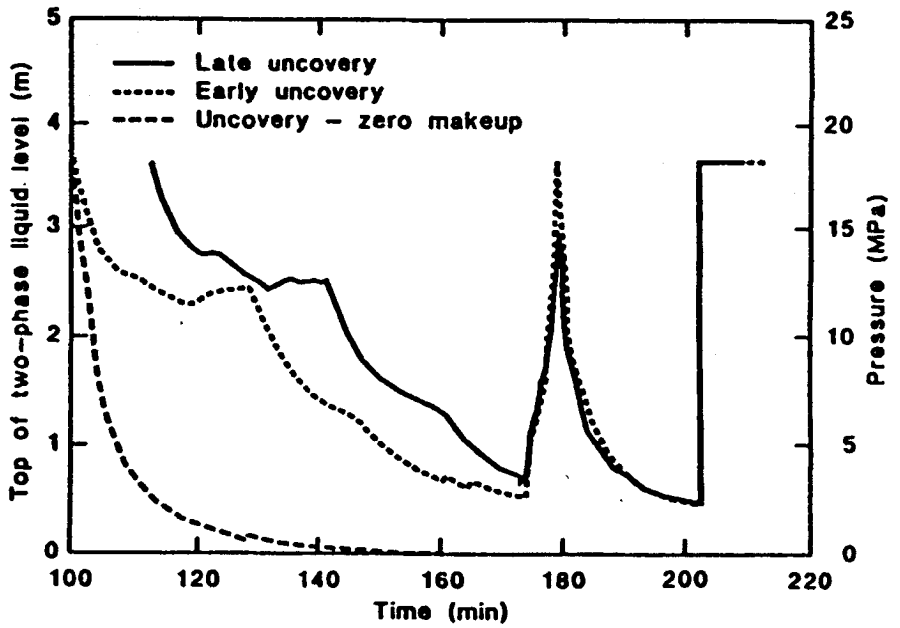


Fig.13 : Core uncovery scenarios with TMI

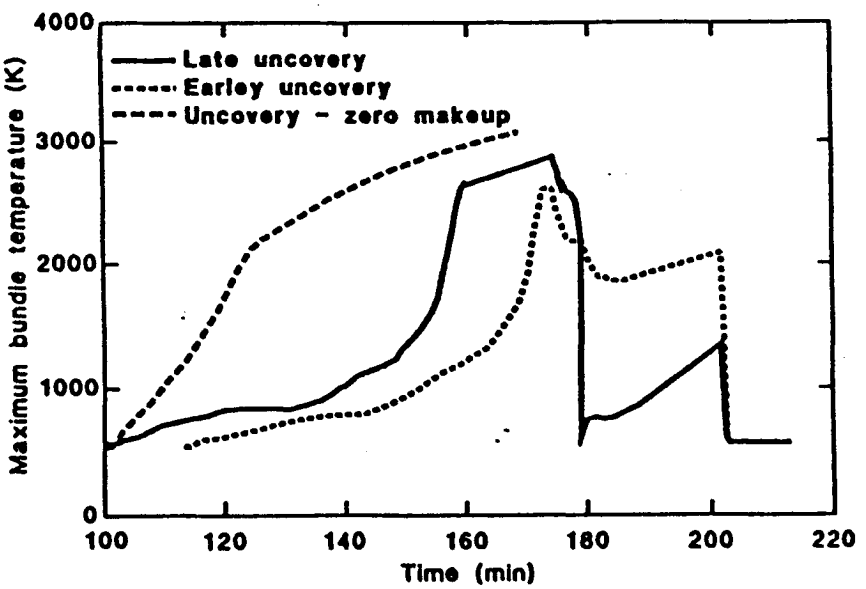


Fig.14 : Comparison of maximum core temperatures for different uncoveries

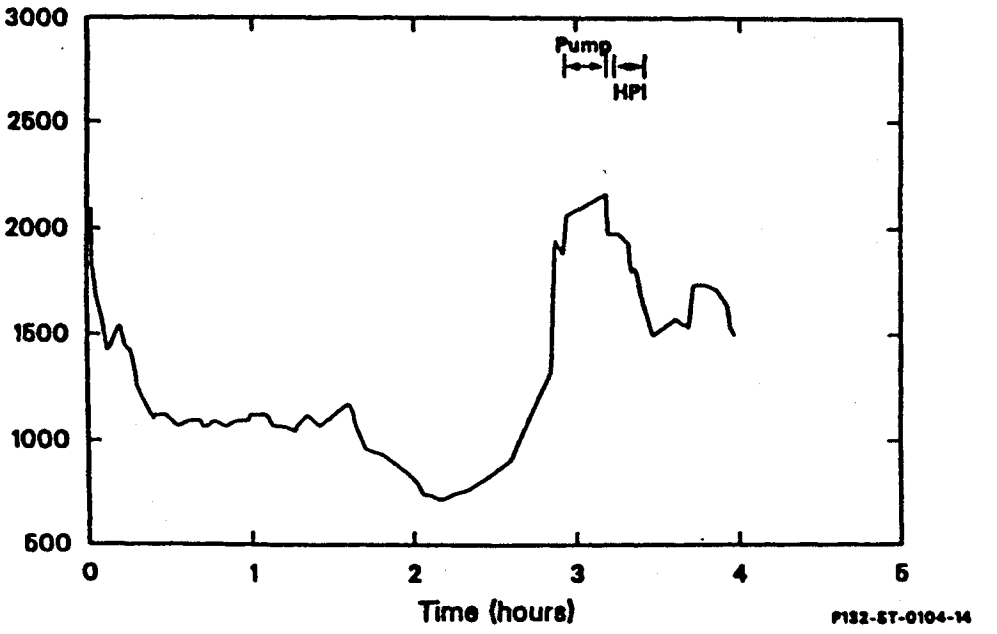


Fig.15 : TMI, Measured reactor system pressure history

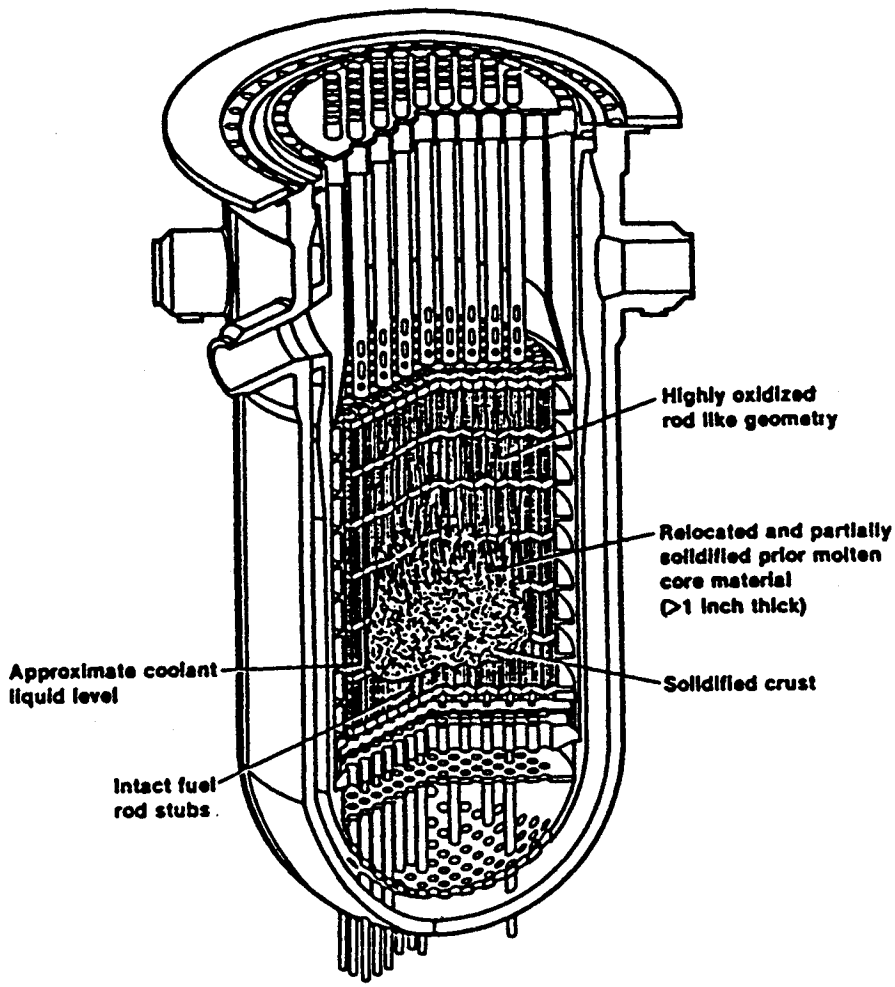


Fig.16 : Core condition just prior to 'B' pump transient (174 minutes)

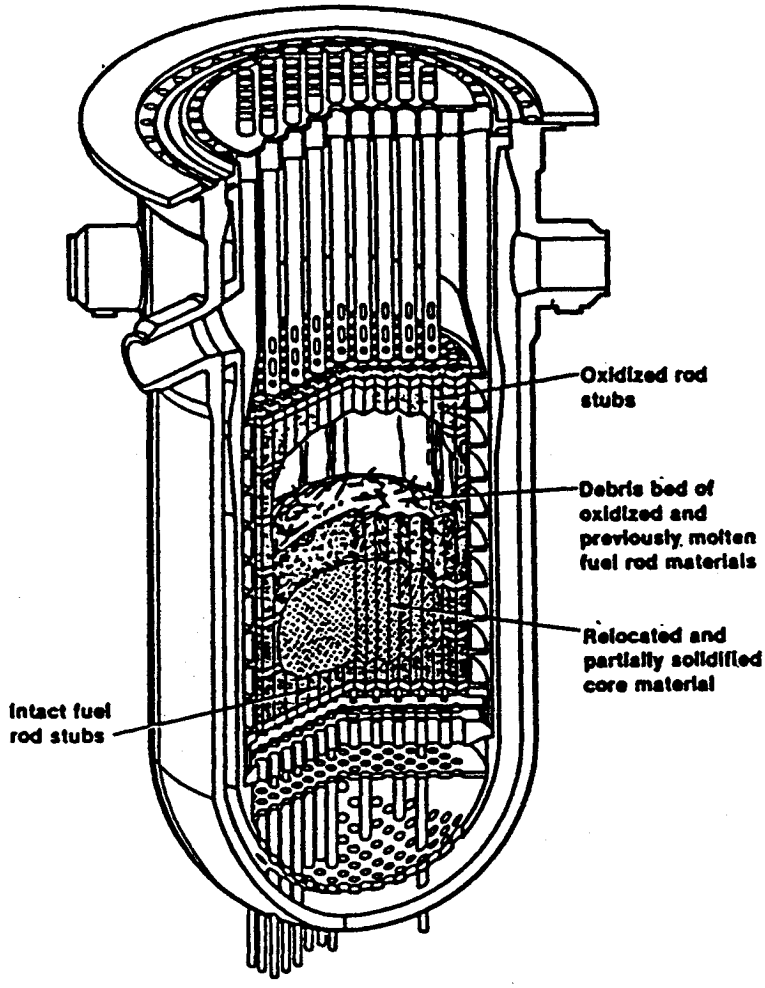


Fig. 17 : Core condition just after 'B' pump transient (175-180 minutes)

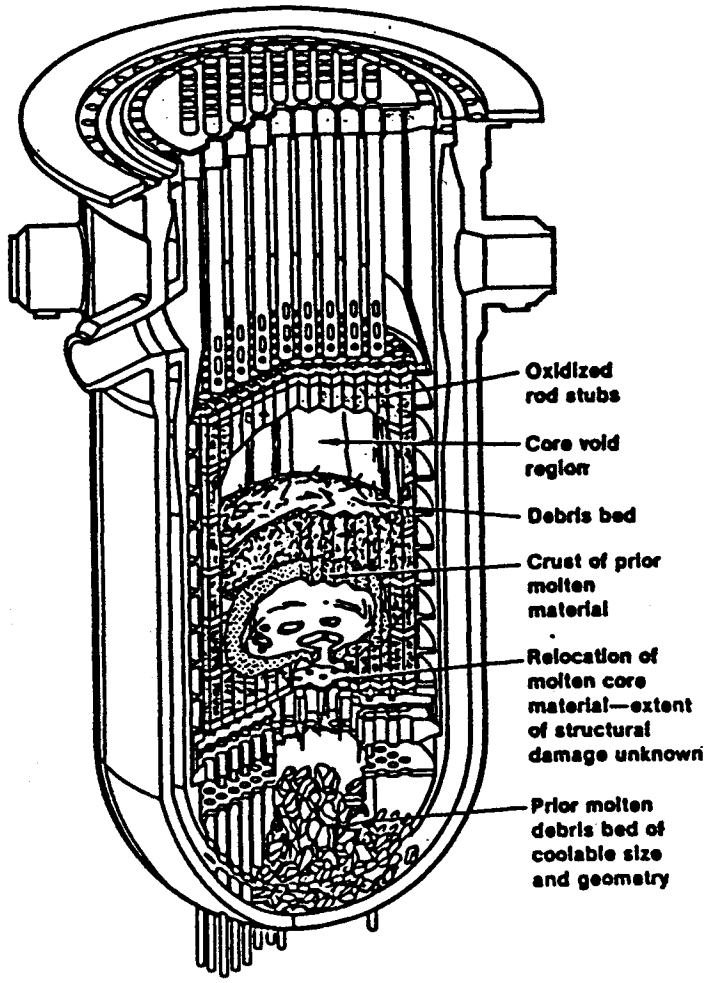


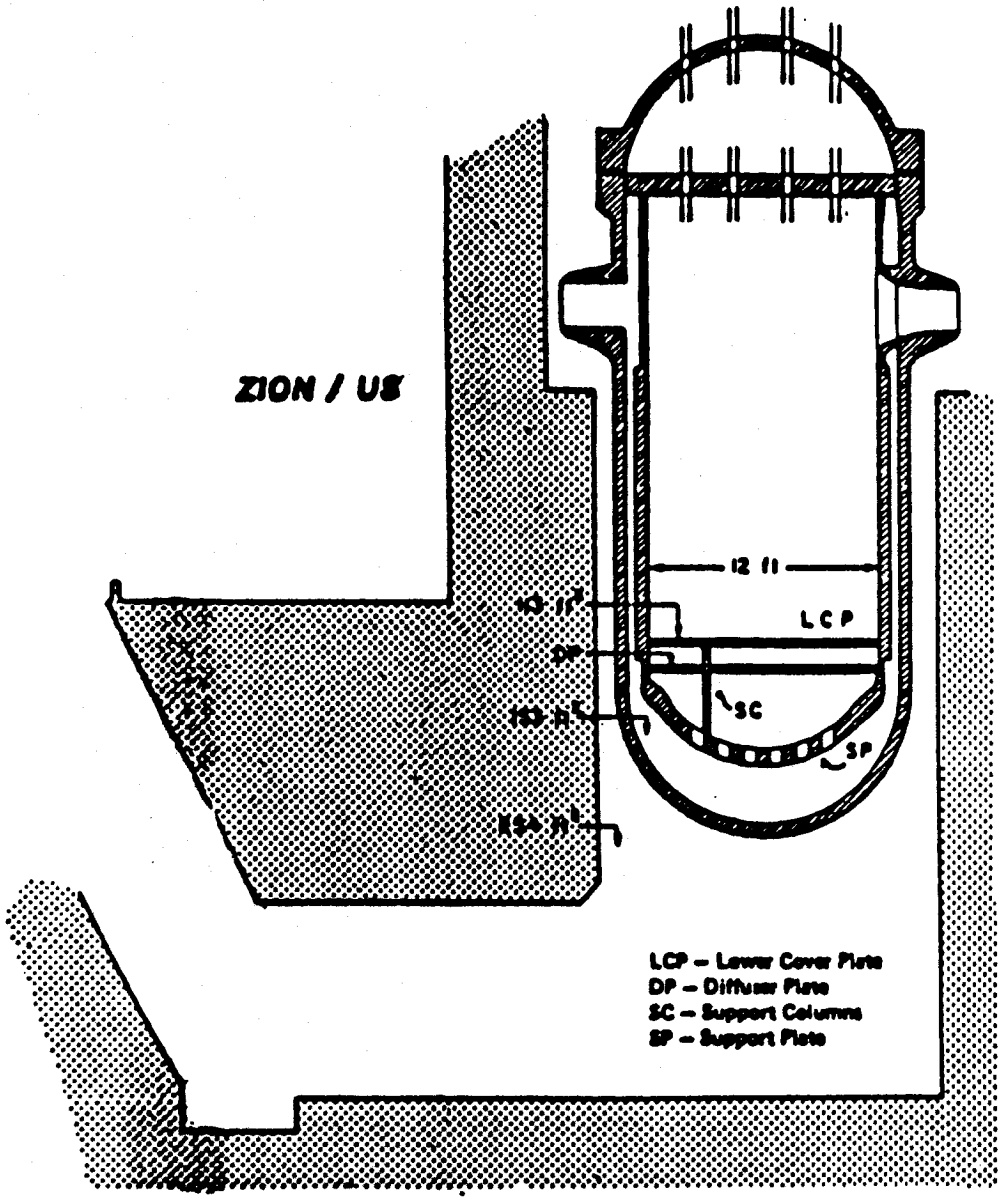
Fig.18 : TMI estimated end state core conditions

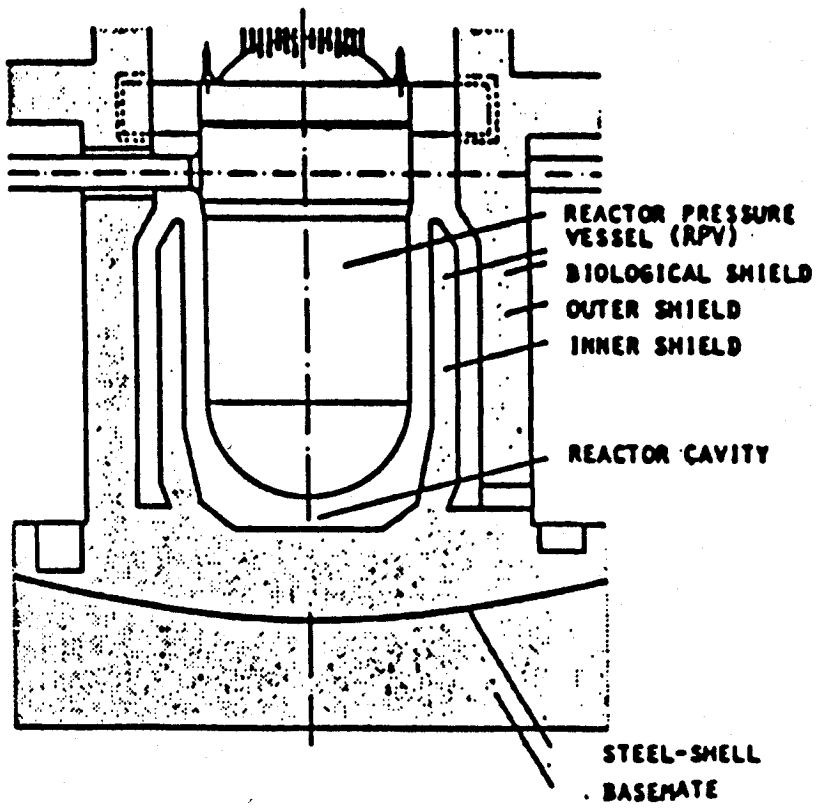
- No apparent damage to upper plenum structures
- Some melting and oxidation of upper grid assembly
- Peak temperatures of 2900-3100 K in upper rubble
- Breakable crust at the 80-90 inch core elevation
- Hard stop at 65 inch core elevation (from probe data)
- Significant fuel liquefaction/melting and relocation. Estimated fuel inventory in lower plenum region may be as high as 20%

Fig.19 : Summary of damage (TMI)

- Damage to the lower core support structure is not known but may be extensive near the core center
- The central 1/3 of the lower core region may have significant voids and rod stubs may exist near the core periphery
- The reactor pressure vessel integrity was maintained
- Progression of the accident was terminated with cooling water from the HPIS
- The postulated accident scenario is consistent with the general trends of the TMI on-line data, known core conditions, severe core damage experiments from the PBF, and best-estimated calculations of the accident

Fig.20 : TMI-Conclusions





BIBLIS B / FRG

Fig. 21 : Different typs of reactor cavities

	Low pressure case	High pressure case
Start core uncovery	0.7 h	2.4 h
Start core melt	1.1 h	2.8 h
RPV failure	2.5 h	3.2 h
Sump contact	6-8 h	3.2 h
Failure Containment (pressure 8.5 bar)	> 4.5 d	4.0 d

Fig. 22 : Time history of core melt accident

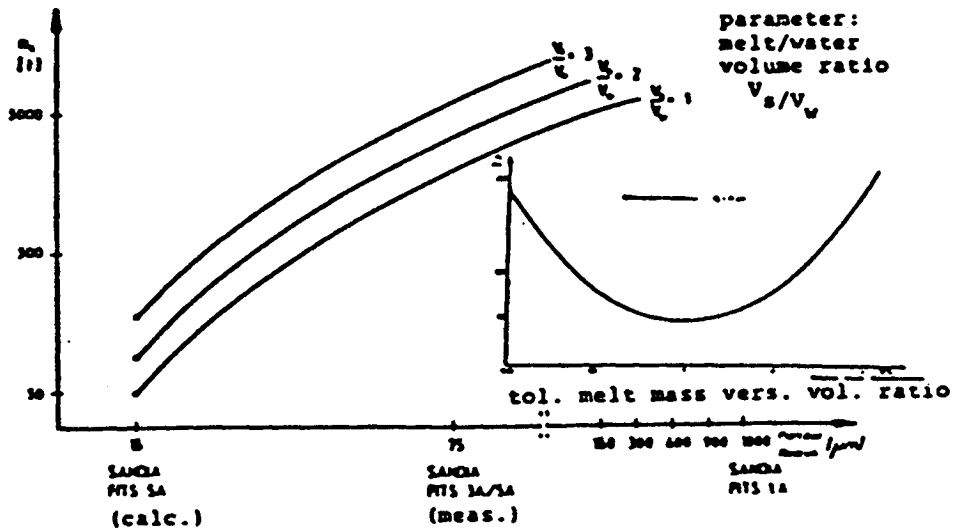


Fig. 23 : Tolerable melt mass for steam explosion in the pressure vessel of the German 1300 MW design (low-pressure core failure case)

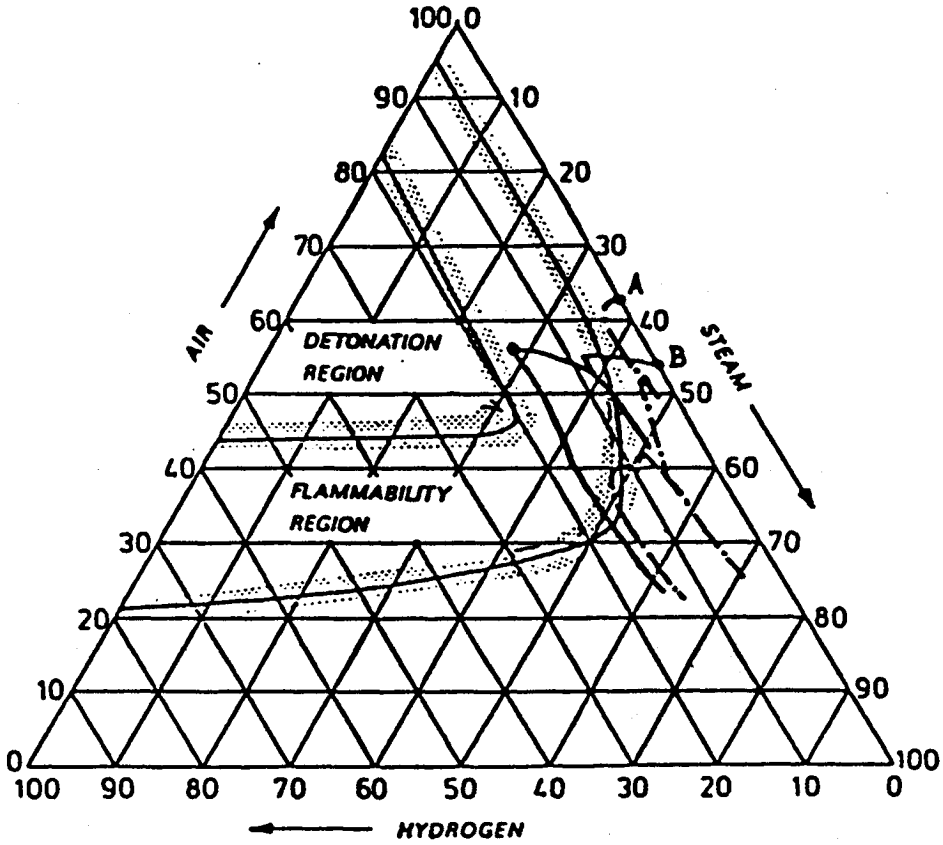


Fig. 24 : Hydrogen enrichment within containment Atmosphere (high and low pressure case, Main assumption : Homogeneous mixture)

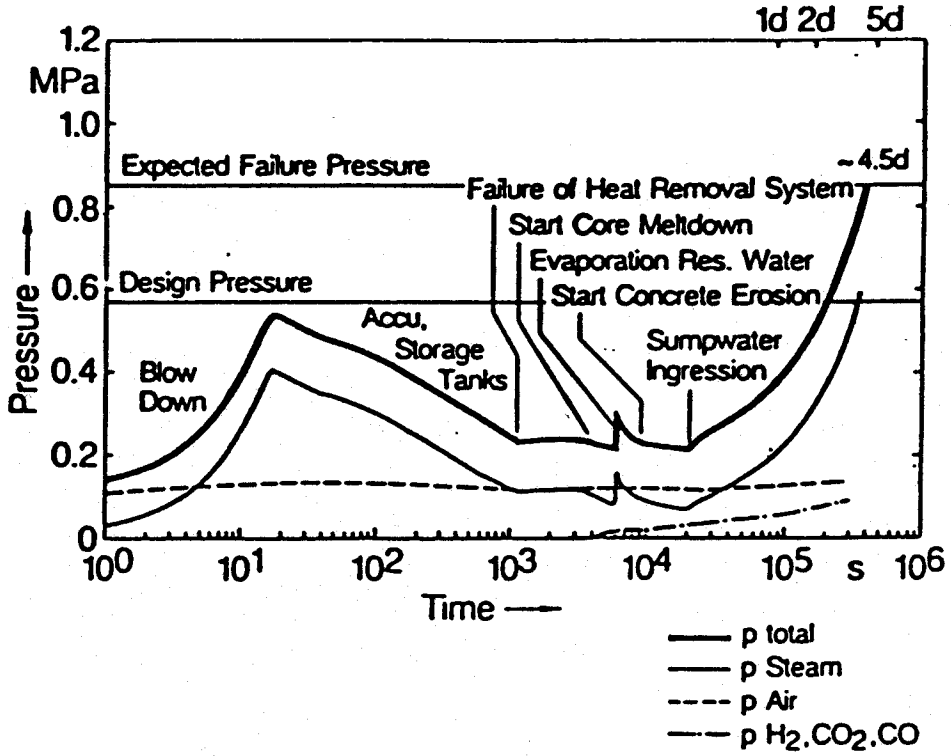


Fig.25 : Containment pressure-time history (Low-pressure case)

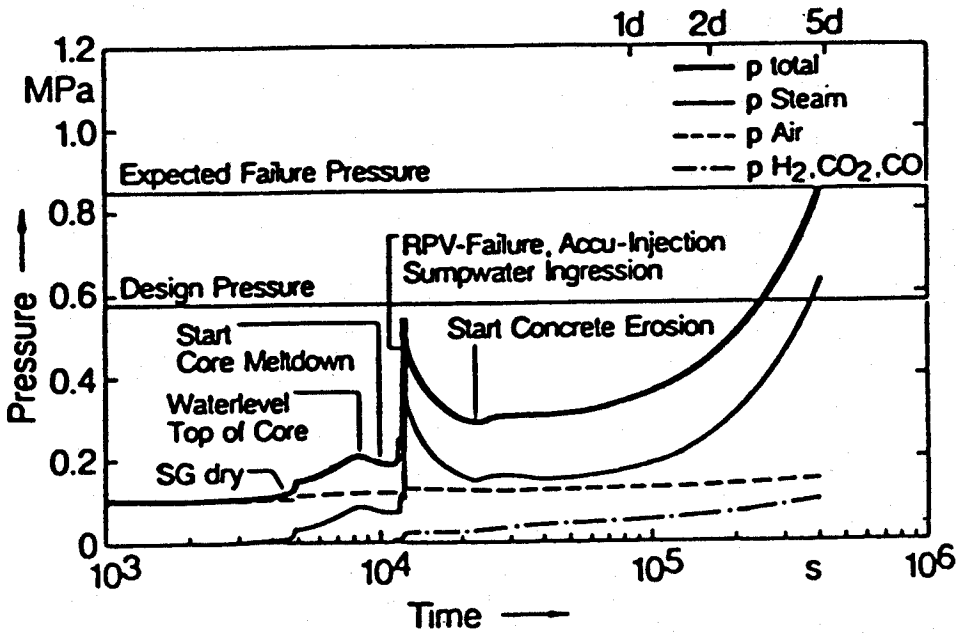


Fig.26 : Containment pressure-time history (High-pressure case)