FUTURE TRENDS IN REACTOR SAFETY

F. Mayinger und W. Riebold

Lehrstuhl A für Thermodynamik
Technische Universität
Arcisstraße 21, 8000 München 2

Abstract

Risk studies and the accidents in Three Mile Island and in Tschernobyl influenced the trends in nuclear safety decisively. While licensing was based in former years mainly on the so-called Maximum Credible Accident, now a catastrophic failure of the reactor core, the possibilities for its prevention and for the mitigation of its consequences, are in an intense discussion. The human factor in nuclear safety plays an important role too.

In the future more emphasis will be given to potential of accident management procedures with the aim to use it for preventing and mitigating the consequences of severe accidents. So the extent of automatic control of safeguard and emergency measures has to be balanced with possibilities for the operator to intervene in the incident sequence by activating cooling- or feeding-systems which do or do not belong to the safeguard- or emergency-systems.

Since the consequences of a nuclear accident affect several countries internationally harmonized rules for licensing and judging of the safety standard of a nuclear reactor would be of great help. With the exception of the fast breader new reactor concepts like an Advanced Pressurized Water Reaktor, for example, will not play a major role in nuclear safety discussions during the next years.

1. Deterministic and probabilistic approach in nuclear safety considerations

In the past licensing of nuclear power plants was mainly based on the Maximum Credible Accident (MCA) which per definition was a break of a large pipe in the primary system. All events beyond this situation were not taken in account. Beginning of the seventieth risk studies like the Rasmussen study [1] or the German risk study phase A [2] were started which were published some years later. In these risk studies it was clearly shown that accident consequenses beyond the situation of the MCA have a very low probability so that they can be excluded almost certainly but not with absolute certainty. So the term "Maximum Credible Accident" was changed in "Design Basis Accident" (DBA).

This deterministic procedure with licensing of nuclear reactors was well justified in the early years of nuclear engineering due to lack of operational experience and of extensive knwo how. Already the risk studies rised indirectly the question whether a probabilistic procedure including hypothetical accidents and their consequences and overstepping the DBA would be more appropriate for defining safety goals. Probabilistic analysis and risk studies were performed, as mentioned above, long before the accident in Three Mile Island occured and thanks to the extensive international research we have good and reliable knowledge and information how a hypothetical accident can be physically described and also its probability can be estimated. With each risk analysis, however, the question exists how complete the problem can be defined and even if it is defined one has still to ask whether all important events are taken in account with respect to the expected frequency of the event. Finally each risk analysis is affected by subjective elements which must not be interpreted as an arbitrary act but which is due to the more or less extensive experience of the evaluating person.

Therefore, there are many good arguments to stay with the proved deterministic principles for design and safety judgement of nuclear power plants. Main reasons for this are - even after Three Mile Island and Tschernobyl - the accuracy and reliability of the safety judgement and the effectiveness of furnishing the proof. Besides that it is certainly conceivable to elaborate a concept for defining and applying probabilistic safety criteria which may amplify the deterministic rules.

Probabilistic studies, however, are an extremely valuable and important help to find weak points in the plant and by this to improve its reliability and safety. From this it becomes evident that each risk study is relevant for a special plant only because it includes its special design, its degree of redundancy of important components and the quality assurance used for manufacturing and operating this special plant. So it is not permitted to draw conclusions from a risk study elaborated for one type of a reactor under the special conditions of quality assurance in manufacturing and operating to another type, neither in a positive nor in a negative way. Very precisely speaking data of risk studies are closely limited to that plant under investigation.

In a good safety philosophy the aim of highest priority must be to prevent accidents a priori by improving the reliability and reducing the probability of incidents arising from malfunctions of components in the plant and by enforcing the reactor controling system and the safeguard systems of the plant. Therefore the so-called Basic Safety plays an important role. Basic Safety includes a reliable and up-to-date design, a careful selection of the material and a detailed and repeted testing not only during manufactoring but also during operation. By this large leaks and breaks can be excluded with extremely high probability and so the field of interest was concentrated on small leaks and incidents without a loss of coolant, for example a station blackout or external events like earthquakes or airplane crash downs. The risk studies clearly proved that events with small leaks including the opening of a small valve have higher probability which is exemplary demonstrated in Fig.1.

2. Safety strategy

There are many safeguard systems to guarantee the integrity of the fuel elements in case of an incident or accident, for example, a loss-of-coolant accident following a small or large break and there are also systems to prevent that radio activity escapes to an unallowed extent into the environment. An example of engineered safeguards is shown in Fig.2 for a pressurized water reactor. In case of a loss-of-coolant accident (LOCA) following a large break the emergency core cooling system and, mainly, the accumulator injection and the low-pressure pump injection in this system play the dominant role in removing heat from the core and in cooling down the core. With small leaks or with transients without a leak the secondary side of pressurized water reactors is vitally important for safety because the heat is transported via natural convection within the primary system from the core to the steam generators where the secondary side is depressurized, and boiling occurs in the secondary fluid. The high pressure pumps of the emergency core cooling system have to replace the water which escapes from the primary system through the leakage. German nuclear power stations are equiped with four independent strings for emergency core cooling as shown in Fig.3. Each of these strings consists of two accumulators, one low-pressure and one high-pressure pump. The design of these strings was made in such a way that one string would be enough to keep the temperature of the fuel rods within a limit prescribed by the safety criteria of the licensing procedure.

There is even a higher redundancy for heat removal from the core during a small leak. As mentioned, the heat is transported via natural convection to the steam generators where, by opening the pressure-relief valves, boiling starts of the secondary-side water, transporting the heat out of the primary system. This evaporated secondary-side water has to be replaced by feedwater systems. As one can see from Fig.4 these feedwater systems have a very high redundancy. Besides the operational feedwater system with the main condensate pumps and the main feedwater pumps, additional feedwater systems are available. The operational feedwater system consists of three independent strings. One of the additional feedwater systems is the start-up and shut-down system with two pumps. The second additional system is the emergency feedwater system consisting of four independent strings, each equipped with a separate emergency feedwater pump which is driven by a Diesel-generator. One of these pumps - either one of the three main feedwater pumps or one of the two start-up and shut-dwon pumps, or one of the emergency feedwater pumps - would be enough to guarantee that enough water is supplied to the steam generators and that the reactor, in case of an accident, can be kept in a safe condition.

One has to mention that the redundancy of heat removal systems is not for all reactors on the international market as high as it is shown in the Fig.3 and Fig.4, which give an example of new pressurized water reactor types, manufactured and operated in the Federal Republic of Germany.

2.1 Classification of hypothetical accidents

Beyond the "design basis accident" one can distinguish three categories of hypothetical accidents as classified in Fig.5. 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 rods remaining within the temperature limit of 1.200°C, as stated in the international guidelines. Here we have to recall the fact that licensing analysis up to now is usually based on conservative assumptions. Doing a best-estimate analysis, one realizes that the maximum cladding temperatures are predicted much lower than under conservative aspects (Fig.6 and Fig.7). The main difference between conservative and best-estimate prediction is resulting from the assumption in the licensing analysis that one of the 4 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. So the capacity of only one and a half emergency core- cooling strings are actively available for temperature reduction of the fuel elements and for decay heat removal (Fig.6).

As mentioned, in the case of a small leak the heat from the core is removed via free convection to the steam regerators 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 may have the consequences of severe core damage, but by reinforced cooling, however, a long-term decay heat removal can be achieved and the core can be cooled down again. The Three Mile Island accident belongs to category II.

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

Before such a situation could occur many barriers would have to fail which are built up and arranged in a modern safety strategy following the principle of defence in depth. In case of a failure in the power line of the station, for example, the turbine will be automatically controlled down to the internal power level at first. Should this procedure not be successful at least two independent feeding lines of electrical power coming from outside and not being interconnected with the power line going outside will supply electrical current to the emergency systems such as the feedwater pumps. If this supply from outside would also fail four Diesel engines are available of which in an emergency case only one would be needed. The safety philosophy for providing this redundant number of Diesel engines is that in the case of an emergency situation one of this Diesel engines would fail and another one is under inspection. Here one has to mention that the inspection periods are very short with respect to the time of availability of these engines. Electrical power in this special emergency case is mainly needed for providing feed-water to the secondary side of the steam generators. If none of the four Diesel engines should start which is extremely unprobable there are in addition the four emergency feedwater pumps available each of which is equipped and driven by its own Diesel engine.

Modern trends in nuclear safety must and will strengthen these strategies of basic safety and defence in depth. First and principle aim of nuclear safety strategy must be to prevent an accident, i.e. to install diverse and redundant systems which guarantee that a fault or disturbance during the normal operation may develop via an incident to an accident. The first system within the strategy of depth to guarantee this is the normal controlling system. If this should not be able to handle the problem the safeguard systems have to interfere and finally the emergency systems have to become active. Each of these systems again consists of diverse and redundant components. One must now ask what happens or wich further possibilites exist if the whole chain of these controlling-, safeguard-, and emergency-systems would fail. For such situations future discussions on nuclear safety philosophy should think about how accident management measures could build up a further barrier against catastrophic consequences of a nuclear accident. As it will be shown in the next chapter there is enough time until a category I accident (which we should better call incident) develops via category II to a category III accident having the consequences of a complete core melt down.

3. Accident management and man-machine-interaction

Each hypothetical accident starts from a situation where for a certain time period conditions of category I exist. The duration of this period is increasing with decreasing leak size, as Fig.8 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 within a man-machine-interaction. For a proper and correct action of the operator in the 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 accicent.

To fulfil the first condition a further improvement of the instrumentation giving information about the cooling conditions in the core is necessary. Therefore, an incore water-level measuring device was developed in the Federal Republic of Germany and was, after testing, installed in all pressurized water reactors. Boiling water reactors anyhow give good information about the water- or swell-level in the pressure vessel. By this the operator has a simple but reliable and comprehensive information about the cooling conditions and the configuration of the core. There is no need for him to combine and to conclude from several indirect informations such as pressure or neutron- flux onto the core conditions.

For matching the second condition the operator needs an excellent training in which he learns to overcome situations for hypothetical accidents. This means that in future trends of nuclear safety the training on simulators plays an important role. New, much more sophisticated simulators have to be developed which are able to imitate the sequences of possible incidents and accidents and to respond on an operator action in a realistic way. These simulators will be mainly based on very large computers working with a parallel satelite system and being equiped with a very fast program being able to simulate the accident situations in real time. Emphasis in future nuclear safety activities, therefore, have to be put on the development of such programs to train the operator in order to enable him to react in a proper way during the time available within the category II period

A category II situation would mean that the emergency core cooling systems or, in case of a small leak or an accident without leak, the feed-water-systems would fail for a certain period of time which may have the consequences of core damage but by reinforced cooling a long-term decay heat removal can be reached and the core can be cooled down again. Sequences of the Three Mile Island accident fit with this category II.

In Fig.9 the tolerable activation delay of heat removal systems for large-break situations is tabulated. The first line 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 exceedes a value which would mean that core melting starts. This is assumed to be by 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.10. Due to easily understandable physical reasons the response-time of these signals is a function of the leak size, as also shown in Fig.10. Looking at this figure we have to realize that for very small leakage sizes - smaller than 1,5 cm diameter - no emergency core cooling system is needed because the volume control 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 blow down even if only one high-pressure safety injection pump would be available.

As shown in Fig.11 the tolerable delay of secondary side blow down activation goes up to 3 h for one safety injection pump and reaches 5 h 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.

One incident of higher probability is the so-called station blackout. In this case no leak exists in the primary system a priori. The decay heat from the core has to be removed, as mentioned above, via the steam generators by blowing down the secondary side of the steam generators. This blowing down is activated automatically and also controlled automatically with a gradient of 100 K/h. All safeguard and emergency measures within the first half of an hour are automatically activated and operated. No manual interference from the operator is possible during this time. The reason for this is that one has to suppose a rather confused and nervous situation in the control room with badly informed operators.

The heat transport from the primary to the secondary side needs no pumping system because free convection will install automatically which is active even with a two-phase mixture in the primary system also containing non- condensible gases due to fission product release. Power is only needed for opening the pressure relief valves on the secondary side of the steam generators which comes from a battery system in case of a total loss of the alternate current system. In addition alternate current power is needed for driving at least one of the feed- water-pumps at latest within 1 hour after opening the pressure relief valves. During this procedure the primary system will stay for a long time under high pressure.

Assuming now in an arbitrary train of thought that all secondary side feed-water-systems fail the steam generators would become empty within approximately half an hour to one hour, and from that on the pressure and the temperature in the primary system would rise. This would go on until the safety valve of the primary system opens, automatically, blowing steam into the containment. Future discussions on nuclear safety trends should concentrate on possibilities to prevent the core from melting even in such a situation. One of such possibilities would be to open existing or newly installed pressure relief valves and to blow down the primary side into the containment before the safety valve would open automatically. The flashing produced by this blow down lowers down the temperature of the primary water, enables boiling in the core and by this removes heat from the core which is blown in the form of steam into the containment. This, certainly, has the consequence of a loss of water inventory in the primary system. Within approximately one hour the water level in the primary system would be down to the upper head of the core. Therefore one has to activate water injection in the primary system again before the upper parts of the fuel elements run dry. A simple and safe way to do this is to blow down the primary system fast enough to a pressure below 26 bar at which the accumulators automatically open and feed their water inventory into the core. This water mass of the accumulators is sufficient for more than 5 hours boiling and by this removing decay heat from the core. Thus the operator has more than 5 hours time to activate one of the components of the emergency core cooling system either a high-pressure injection pump or, if the blow down continues to below 8 bar, one of the low-pressure heat removal pumps.

With cladding temperatures of fuel elements above 800°C a comprehensive hydrogen production would start due to the chemical interaction of the steam with the zirkon. This hydrogen forms an explosive atmosphere in the containment. Therefore, measures should be discussed how to recombine this hydrogen to water or how to burn it without endangering the containment shell. German water-cooled reactors have installed recombining systems which can overcome this problem up to a certain hydrogen production. In case of a severe core melt situation - category III accident - their action, however, would be not powerful enough to avoid an explosive situation in the containment. Therefore deliberations taking into account new trends of nuclear safety should deal with possibilities of developing and installing more powerful hydrogen recombiners, for example by catalytic means in form of huge plates covered with a catalyst.

For boiling water reactors there was a decision of the German Reactor Safety Commission some weeks ago that the containment atmosphere has to be filled with an inert gas to avoid ignition. With pressurized water reactors having a much larger containment than boiling water reactors filling with inert gas would deteriorate the overall safety rather than to improve it. The reason is that during normal operation the different compartments of the containment of a pressurized water reactor are inspected so that any failure of primary circulation pumps or of any other active component can be early detected before an incident occurs. This is in the sense of the nuclear safety philosophy: to prevent accidents rather than to mitigate their consequences.

4. Mitigation of accident consequences

Before discussing possibilities of mitigating severe accident consequences we have to see how such a severe accident - category III accident - would develop and how radio-activity would be emitted into the environment.

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.11. This time history would be only relevant if no depressurization of the primary system as explained in chapter 3 would be initiated. With such a depressurization 5 more hours would be available to act against the accident sequences before the core melt would penetrate the pressure vessel. This is due to the water inventory in the accumulators which becomes available for heat removal from the core.

In the following discussion we will assume that this depressurization is not activated. Then there would be only a small difference in time until the melt would come into contact with the water in the containment 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 radio-active material could escape into the environment to a not permissible extent:

- steam explosion
- penetration of the core foundation

- hydrogen explosion or detonation
- over-pressurization.

There were and are long discussions whether a steam explosion - which is a thermal interaction between liquid molten corium and water - can distroy the containment or even the pressure vessel. Two situations are imaginable in which an explosion-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 of the pressure vessel. In case of a small leak or station blackout this situation of flowing melt into the water of the lower plenum would need an extremely high triggering energy due to the high pressure situation as we know from steam explosion experiments reported in the literature [3]. Here is to mention that during the Three Mile Island 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 into contact with the 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 the melt will creep under the water. 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.13 - because there is a dry cavity under the pressure vessel.

From the detailed experimental and theoretical studies one can draw the conclusion that a steam explosion powerful enough to destroy the pressure vessel of a nuclear reactor would need such a large amount of melt which, under physically realistic assumptions cannot be provided in such a short time as steam explosion conditions would necessitate. With regard to steam explosion we have to realize that only a few seconds are available for a large amount of melt which has to be homogeneously premixed with water without strong separation effects which may be possible only for a few hundreds kg of melt. However, for endangering the pressure vessel or the containment several tons of melt would have to be homogeneously premixed with water. During this premixing no major part of the melt is allowed to freeze because frozen particles cannot react in a steam explosion. Furthermore there must not be any boiling during this premixing period.

There are accidents reported in conventional engineering especially in foundries where a steam explosion blew off the roof of a manufactoring hall. However, here we have to realize that a manufactoring hall will be destroyed by a pressure shock of a few tenth of a bar while the containment of a pressurized water cooled nuclear reactor can withstand 9 to 12 bar.

It is very likely that small steam explosions would occur during a core melt down when the melt interacts with water. These small steam explosions do not harm the containment or the pressure vessel but they are the best guarantee that no melt-water-mixture can be collected being large enough for a powerful and dangerous steam explosion. Therefore the destroyment of the containment wall by a steam explosion can be excluded even in a severe core melt down accident.

Due to the safe design against earthquakes and against events from outside, like airplane crash-down or explosions of chemical clouds in the atmosphere, the concrete foundation of German pressurized water reactors is very strong. Therefore, it would take days until, after a catastrophic failure of the core, the melt could penetrate this concrete foundation. Much of the radioactivity being present in the melt at the beginning of the accident would have abated. Especially the highly volatile components of the core would have already escaped out of the melt into the gaseous atmosphere in the containment. Experiments have shown that after penetrating the concrete foundation the melt would freeze latest in the soil forming a rigid shell of condensed solid material around 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.

In case of a core melt down hydrogen would not only be produced by the chemical reaction between water and the zirkon of the cladding and the structure material in the pressure vessel but also by the heat attack and the chemical reaction with the iron in the concrete foundation. So the amount of hydrogen being present in the containment after a core melt down would be much larger than that discussed in the previous chapters.

The hydrogen can react with the oxygen of the air in the containment in a deflagrative or in a detonative way. Hydrogen deflagrations occurred, for example, during the Three Mile Island accident. They produced no major damage there.

Experiences from experimental and analytical research allow to draw the conclusions that a deflagration would endanger or damage the containment only in a very unlike case. Most of the containments of pressurized water reactors could withstand even a strong hydrogen-deflagration. The situation would be much more unfavourable if a combustion starting in a deflagrative way could be accelerated to a detonation by turbulent mixing in the flame front. However, experiments by Brehm [4] showed that with a steam content in the containment atmosphere of more than 35% a detonative combustion even with strongest acceleration of the flame front is no more possible. This results from the strong damping effect of the steam molecules acting as inert gas.

Mainly due to evaporation of water - but to a smaller extent also by carbondioxyd 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.14 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.15. The pressure peak around 3 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 their water into the melt. There were no prior depressurization measures assumed as discussed above to prevent the core from melting. 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.15 demonstrates. But in any case after several days the pressure in the containment would reach a value which is not only beyond the design presssure of this vessel but also beyond the failure pressure. A catastrophic failure of the containment due to overpressurization would result in a release of radio-active products near the ground.

In the Federal Republic of Germany long and intensive discussions were conducted whether and what measures should be taken to prevent the containment from a catastrophic failure due to overpressurization and by this to mitigate the consequences of such an accident. Finally there was a decision to install in all containments of pressurized water reactors and of boiling water reactors a relief valve which could be opened during a core melt down accident before the failure pressure would be reached.

In an emergency case, after opening an already existing valve at the containment, the gas-steam-aerosol-mixture would flow via a pipeline to an aerosol filter where more than 99% of the radio- active aerosols would be held back. From this filter the mixture flows via another pipeline to the entrance chamber of the chimney. In boiling water reactors the system of the containment depressurization is similar, only the filter has in addition a venturi scrubber for cleaning purposes because due to the smaller containment volume of boiling water reactors the depressurization has to start earlier, i.e. at a still higher radioactivity level.

To reach an optimum between safe containment integrity and as low as possible environmental pollution the depressurization is stopped when the pressure in the containment reaches approximately half the design pressure. The depressurization is rather smooth, i.e. it can take 1 to 2 days until this lower pressure limit is reached at which the relief valve is closed again. Then intermittent opening and closing periods could follow.

To avoid that the water inventory in the containment is lost by this depressurization, which has a flashing as a consequence, the utilities have to provide an additional water injection device to supply at least that amount of water which was blown out through the pressure relief valve. For a 1.300 MWe pressurized water reactor the design basis for such a pressure relief valve is approximately 3 to 5 kg/s gaseous mass flow rate which guarantees a depressurization from 6 bar to 3 bar within 2 days. To provide the possibility of cooling down the inventory of the containment the mass flow rate of the water injecting system is higher, approximately 10 kg/s.

So future trends in reactor safety will have to deal with the problem whether, how and to what extent it is necessary and advisable to provide techniques and to install safety and emergency components for mitigating the consequences of a severe accident and preventing from a catastrophic failure of the containment. Risk studies will be a great help for identifying which failure sequences should be prevented and which failure consequences can and should be mitigated always taking into account that costs and benifits must be in a certain relation. This is not to be understood in such a way that safety is a question of money but, further more, a risk study is a good help to check which would be the real benefit of an emergency measure. From a theoretical point of view the probability of a hypothetical accident with its core melt sequences and consequences never reaches the value zero even with almost an infinite number of safeguard and emergency systems. However, from a practicle point of view we can assume that an event of enough low probability never will occur. Measures against such an event, therefore, would have no practical benefit, even if their costs would be low.

5. International safety standard

European countries are very densly populated and the distance from border to border is usually small. Nuclear safety deliberations, therefore, have to go beyond the national borders because environmental pollution would not stop at the national border. To guarantee all citizens of all countries in the European continent the same or at least a similar standard of safety an international harmonization of the national rules in the peaceful use of nuclear energy is needed. On the other side this harmonization must not lead to a paralysis in the development of nuclear safety devices due to bureaucratic effects. Harmonized rules furthermore should guarantee an international standard of nuclear safety which depending on the national interests and requirements allows improvements.

There are good internationally agreed rules in nuclear liability and in the radiation protection law. However, there are only very weak and very recent contacts about internationally agreed rules concerning the design, the construction, the operation and the decommissioning of nuclear power plants. Certainly there is a licensing procedure in all national regulations for the construction and the operation of nuclear power plants, however, the details of these regulations and also the standard are different. It would not be sensible and useful to harmonize the formal and administrative procedure in licensing nuclear power plants. This always has to be linked with the traditional national nature of the administration. However, there should be more expert discussions on technical aspects of safeguard and emergency systems and of desired nuclear safety standards. This should not mean that in the near or far future the safeguard and emergency systems are uniform because a diversification would give much more valuable and useful information and would help to gain important experience. A common understanding, however, should be found about the tolerable risk, the standard of instrumentation and controlling devices, the degree of redundancy in safeguard and emergency systems, the extent of automatization in normal operation procedures and in emergency situations and the training of the operating staff.

An international exchange of the knowledge gained from experimental and theoretical nuclear safety research should be promoted and an international cooperation in performing investigations in this safety field should be encouraged. People being active in the research field should have close contact with those being responsible for licensing, and licensing committees should be supplemented by members coming from the research side.

There are several international groups active in this field, mainly within the European Community, the OECD or the IAEA.

Close bilateral or trilateral cooperation exists since many years between the USA, Japan and the Federal Republic of Germany. As an example the so-called 2D/3D-project should be mentioned in which the USA, Japan and the Federal Republic of Germany cooperate and in which large test-facilities are operated in Japan and in the Federal Republic of Germany. The USA provide code development and analytical work and also advanced instrumentation to these facilities. The total costs of this cooperation probably exceed 500 million dollars.

A cooperation in research only, however, would not improve the nuclear standard necessarily. Weak points in each safeguard and emergency system have to be investigated separately. For this probabilistic risk studies are an excellent tool. Such studies, however, are very specific not only for a given reactor type but even for a special plant because the design and manufacturing standard of the components, the redundancy of safeguard and emergency systems, and the operation experience of the staff have great influence. Reliable data of risk studies need detailed and long-time experience with components like valves, pumps or electronic devices installed in the nuclear power plant under study. Insurance companies usually collect such information not only from nuclear but also from conventional plants and an exchange of their know-how could give some progress in doing risk studies in different countries and for plants of different design.

Nuclear safety can be internationally improved also by exchanging operational experience collected during the lifetime of each plant. If information about events and incidents - their cause and their consequences - are collected and evaluated in a central institution very valuable educational aid could be given to all utilities in the international community operating nuclear power plants. Also the vendors could profit from such an exchange of experience. This kind of international information will play an important role in improving nuclear safety and must be a point of emphasis in future nuclear safety philosophy.

6. Advanced reactor concepts

Advanced reactor concepts beiñg already in operation or at least in construction are the sodium cooled fast breeder and the gas cooled high-temperatur reactor. Both types are licensed on a basis and procedure similar to that of light water reactors and requiring the same high level of nuclear safety standard. In the Federal Republic of Germany both, the fast breeder (SNR 300) and the gas cooled high-temperature reactor (THTR 300) are of prototype character being a development basis for future plants. Safety philosophy applied to these reactors took into account the special characteristics and design features. The SNR 300 is provided with an emergency system which is not only preventing hypothetical accidents like a prompt critical excursion with a core desintegration, but also mitigating accident consequences.

Future concepts discussed are small units of gas cooled reactors for electrical power generation as well as for chemical application, district heating plants and a so-called Advanced Pressurized Water Reactor (APWR; Fortschrittlicher Druckwasserreaktor, FDWR). The concept of the latter is not a new design of the total pressurized water reactor but of the core of this reactor type. This newly designed core concept has a very high convertion rate which means that the inventory of water in the core has to be kept to a minimum. Therefore, the distances between the fuel rods are very small. This results in a high pressure drop over the core length. Licensing procedures and nuclear safety deliberations, therefore, mainly have to deal with the possibilities of emergency core cooling of this new concept. Special attention has also to be given to the forces acting on the core during the blow down of a loss of coolant accident with large leaks. It has to be guaranteed that during such a situation the core configuration stands stable enough that the control rods can fall in and shut down the reactor.

There are up to now no formal discussions about any licensing aspects of these future concepts. Starting of the licensing procedure is not before a formal application for constructing and operating such a plant is submitted to the appropriate and reponsible authority. Therefore no authentic information can be given what requirements in detail would have to be fulfilled for such a plant. However, the overall statement is certainly correct that the general standard of safety must be at least as high as that of operating nuclear power stations and that the risk from such a new plant must be as low as that of an existing plant of the latest design.

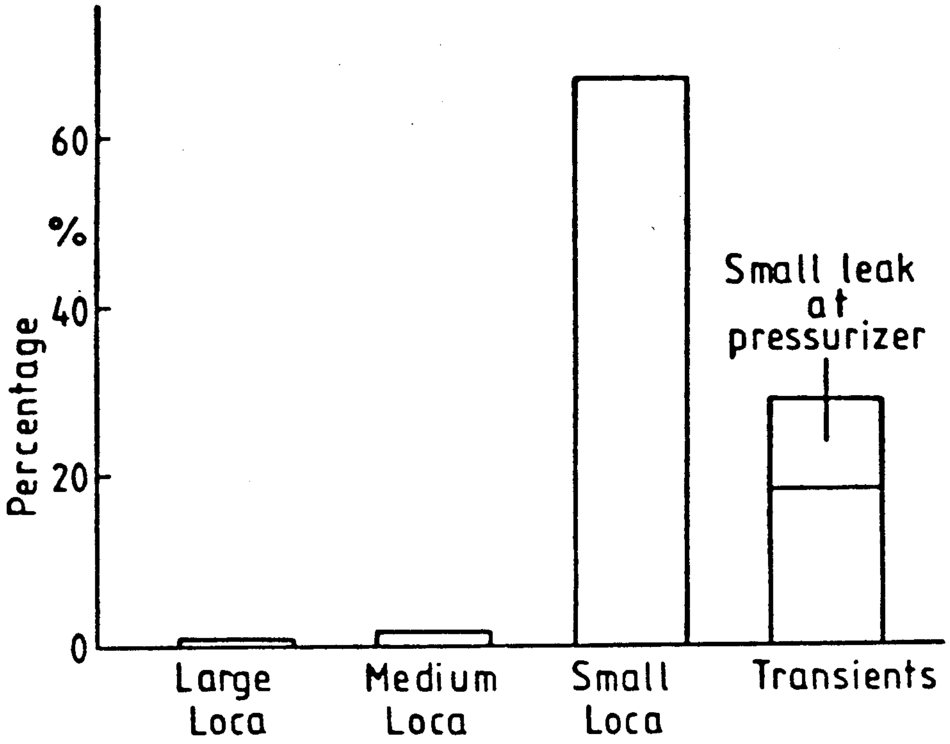
Finally one could philosophize about the safety standard of district heating plants being sited near large cities. There is a rule in the German Constitution that every person has the same rights. So it would be illegal to construct and operate a power plant even in a remote area if the safety of a single person in the neighbourhood would be endangered distinctly beyond the overall risk-level. The collective risk is certainly a function of the number of inhabitants per unit of area. So a risk study for a power plant being sited near a densly populated area such as a city would look more carefully also to contributions to the overall risk from very unprobable events. There was a licensing discussion started several years ago about a pressurized water reactor to be constructed in a chemical factory very near to a densly populated area.

The application for constructing and operating this plant was finally withdrawn by the user. However, many additional safety measures and devices found useful and valuable during this discussion were later on applied to pressurized water reactors being constructed at normal sites.

Presently there seems to be no urgent economical need to intensify the program for constructing new nuclear power plants in the Federal Republic of Germany. Therefore also the situation with respect to licensing advanced concepts like the APWR or a district heating station is rather relaxed. The situation 5 to 10 years from now may be quite different.

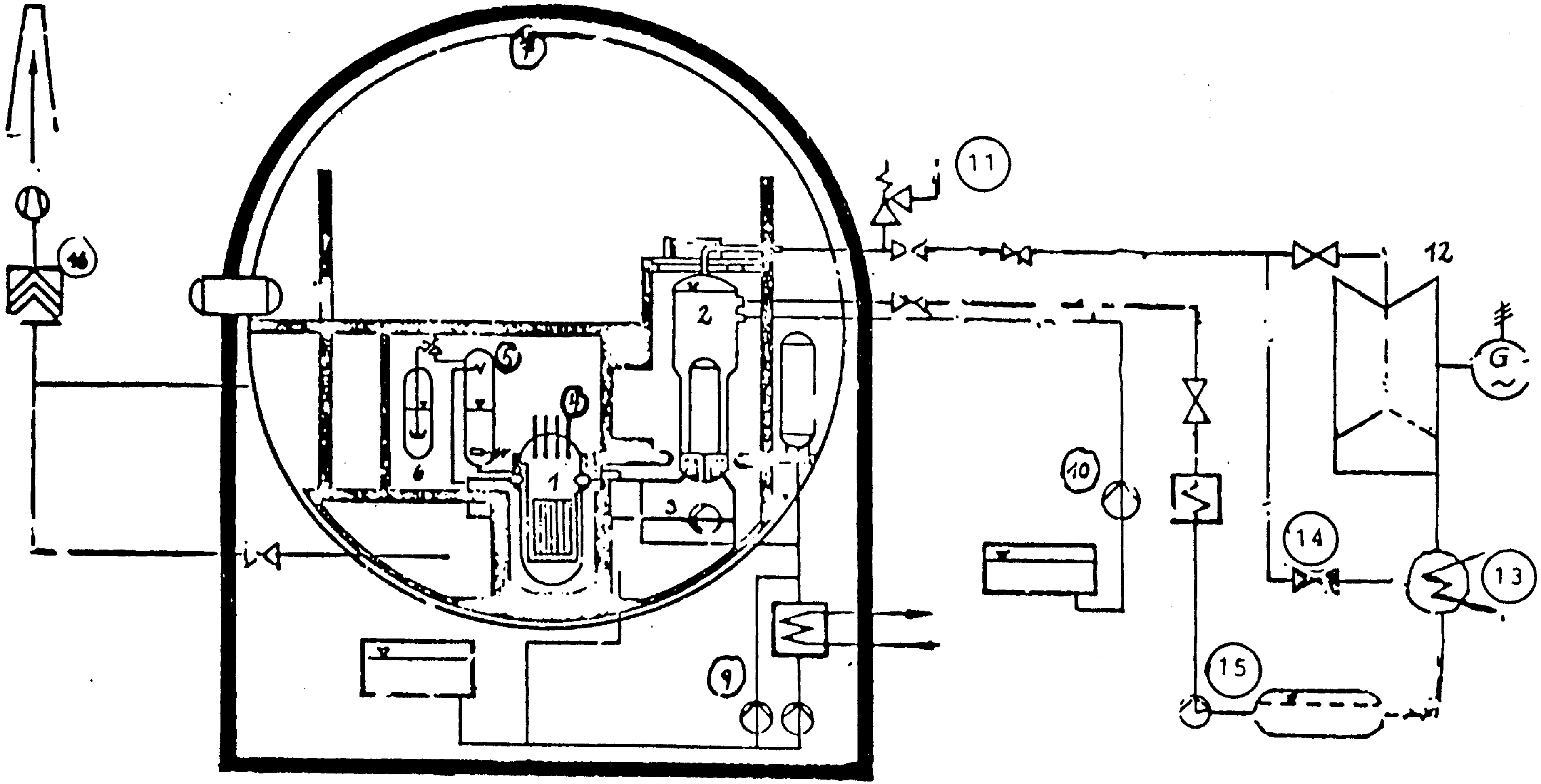
References:

1. Rasmussen, N. C., Reactor Safety Study - An Assessment of Accident Risks in US-Commercial Nuclear Power Plants, USNRC WASH 1400 (NUREG-75/014).
2. Deutsche Risikostudie Kernkraftwerke, Herausgeber: Der Bundesminister für Forschung und Technologie, Verlag TÜV Rheinland, Köln 1979.
3. Bürger, M. u.a., Abschlußbericht zum Forschungsvorhaben BMFT 1500 639 0, Theoretische und experimentelle Untersuchungen zur Eingrenzung von Dampfexplosionen im Rahmen von Sicherheitsbetrachtungen bei Leichtwasserreaktoren, Institut für Kerntechnik und Energiesysteme, Universität Stuttgart, IKE 2 TF-77, Febr. 1987.
4. Brehm, N., Zündgrenzen von Wasserstoff in aerosolhaltiger Atmosphäre des Containments nach Kernschmelzunfall, Abschlußbericht zum Forschungsvorhaben BMFT 1500 615, Lehrstuhl A für Thermodynamik, Technische Universität München, 1986.



Relative contribution of various initiating events to probability of core melt

Fig.1 : RESULTS OF EVENT TREE ANALYSES



1 REACTOR PRESSURE VESSEL WITH CORE
2 STEAM GENERATOR
3 MAIN COOLANT PUMP
4 CONTROL ROD DRIVES
(FAST SHUTDOWN SYSTEM)
5 PRESSURIZER WITH RELIEF
AND SAFETY VALVES

6 RELIEF TANK
7 CONTAINMENT
8 REACTOR BUILDING
9 EMERGENCY CORE
COOLING SYSTEM
10 EMERGENCY FEEDWATER
SYSTEM

11 STEAM LINE SAFETY VALVE
12 TURBINE WITH GENERATOR
13 CONDENSER
14 TURBINE BYPASS
15 FEEDWATER SYSTEM
16 VENTILATION SYSTEM

Fig.2 : Engineered Safeguards of a PWR

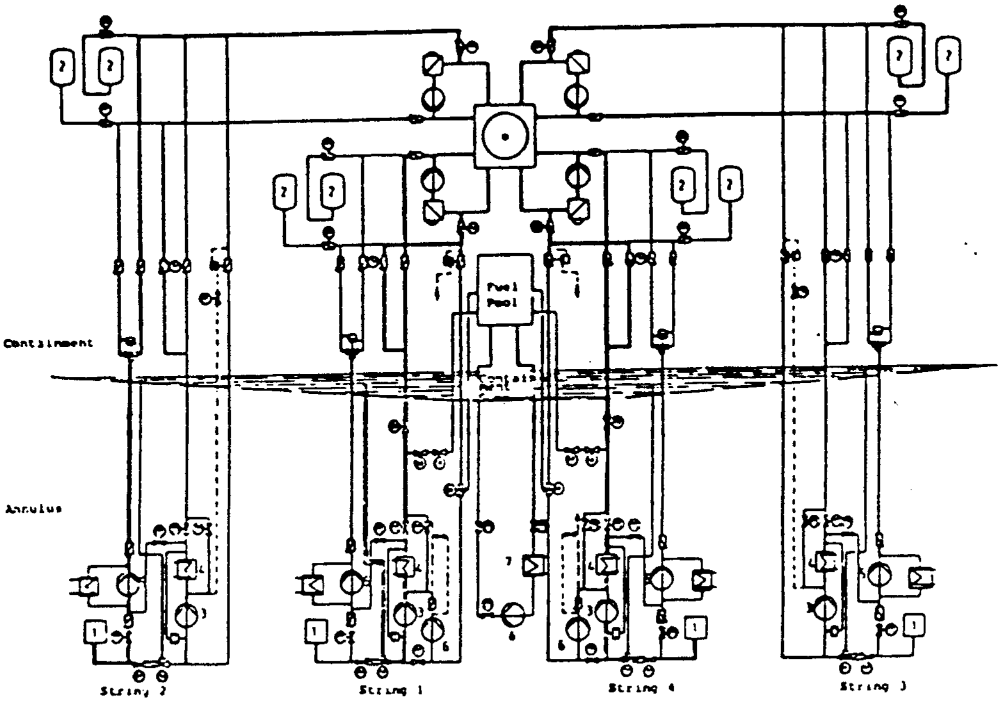


Fig.3 : Residual heat removal system(each string shown in one of the possible operation modes) 1300 MWe 4-Loop KWU PWR

String 1: Sump recirculation mode
String 2: HP-safety injection
String 3: Accumulator injection
String 4: Low pressure injection

1.Borated water flooding reservoir
2.Accumulator
3.Residual heat removal pump (LP-injection pump)
4.Residual heat exchanger
5.HP-safety injection pump
6.Fuel pool cooling pump
7.Fuel pool heat exchanger

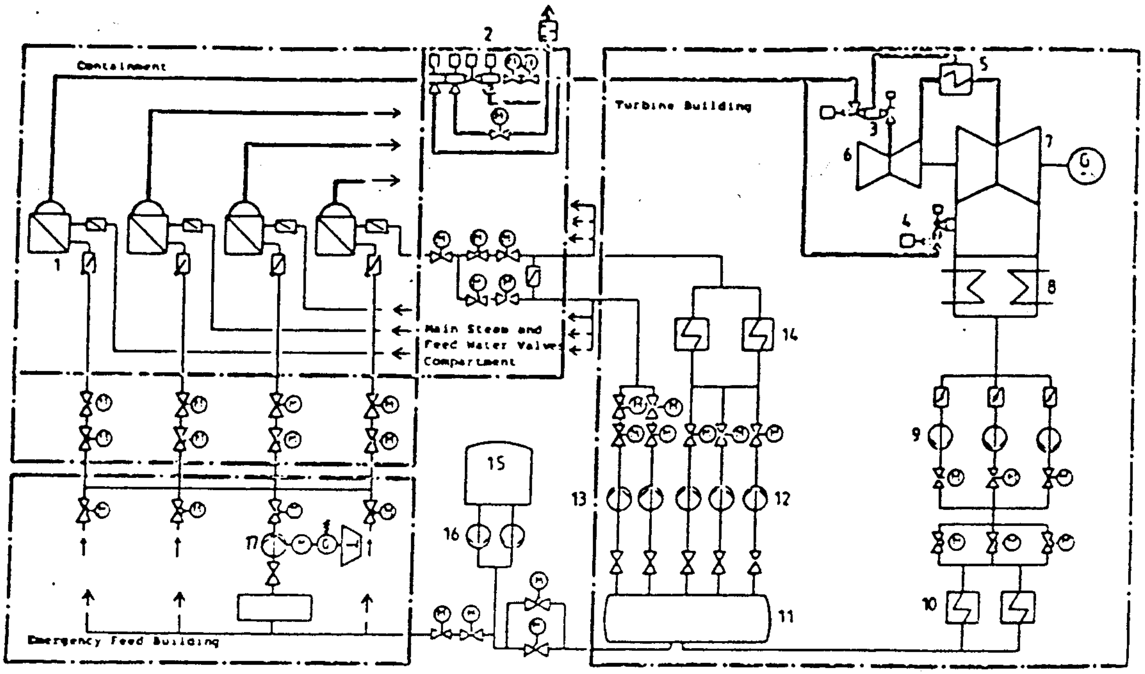


Fig.4 : Main Steam System and Steam Generator Feeding 1300MWe 4-Loop KWU PWR

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

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.5 : Classification of accidents

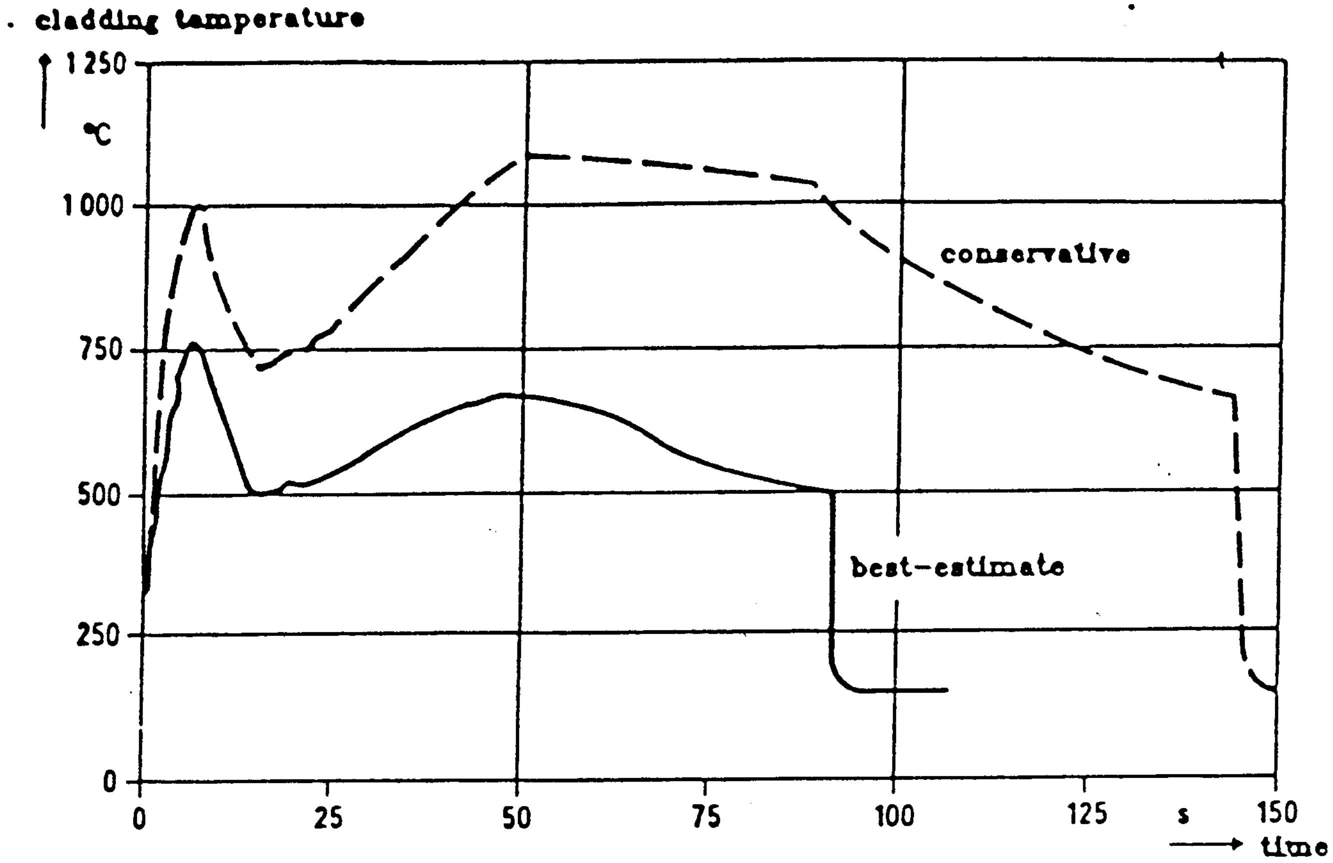


Fig.6 : Cladding temperatures for a hot rod, 1300 MW, PWR, 2 F-break between pump and pressure vessel

	licensing procedure	"best-estimate"
Initial Power	106 %	100 %
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	80 %	100 %
Single Failure and Repair Criterion	yes	no

Fig.7 : Main assumptions for "best-estimate" and conservative blowdown-and reflood-calculations

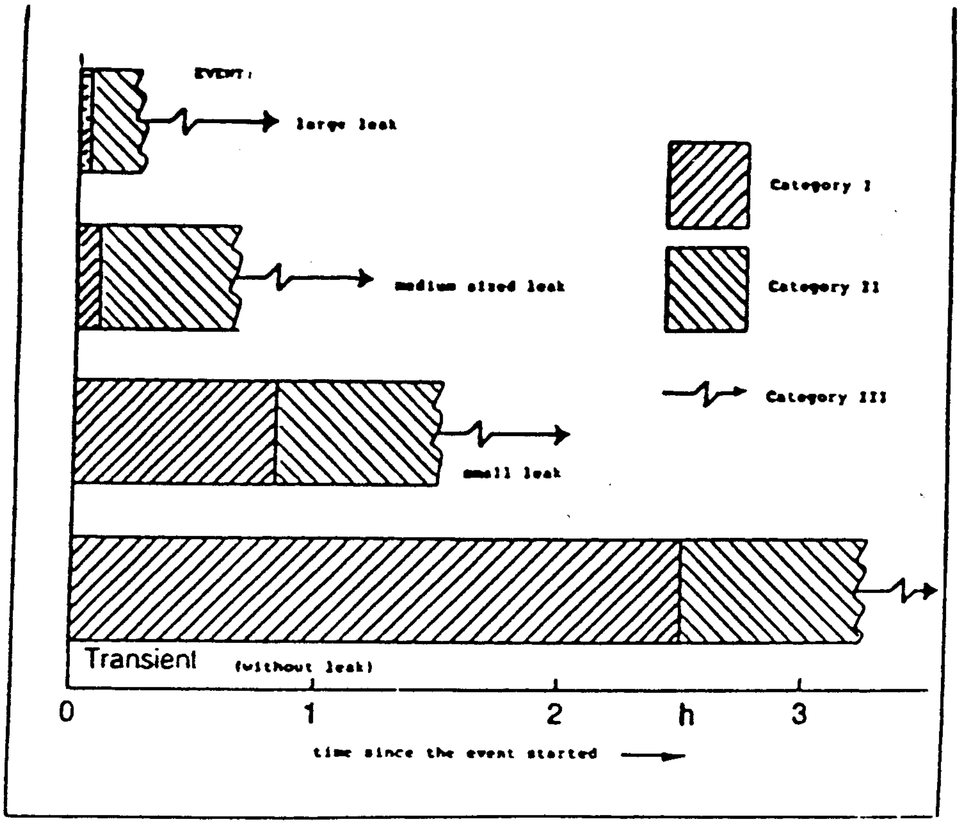


Fig. 8 : Time history of hypothetical accidents and time of tolerance for reinforcing safety systems

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

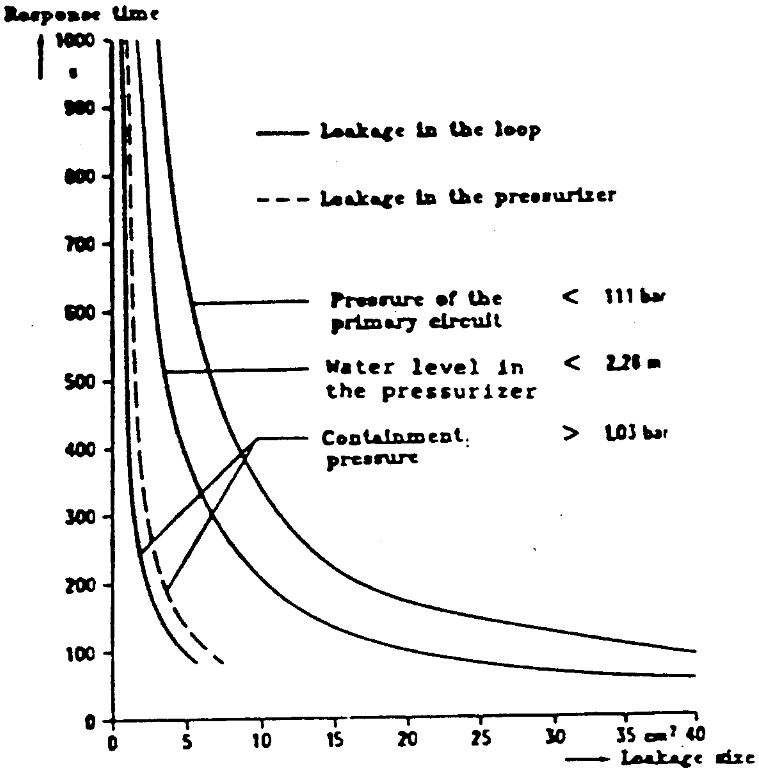
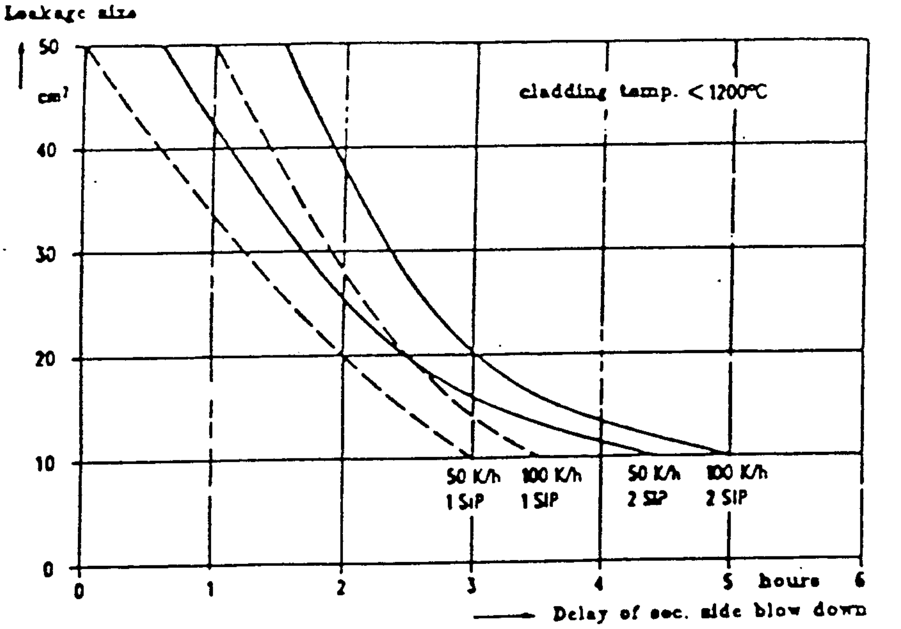


Fig.10 : Response time of safety signals of a 1300 MW PWR



Fic.11 : Emergency cooling analysis in case of reduced system availability and delayed sec.side blow-down (1300 MW PWR)

	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.12 _: Time history of core melt accident

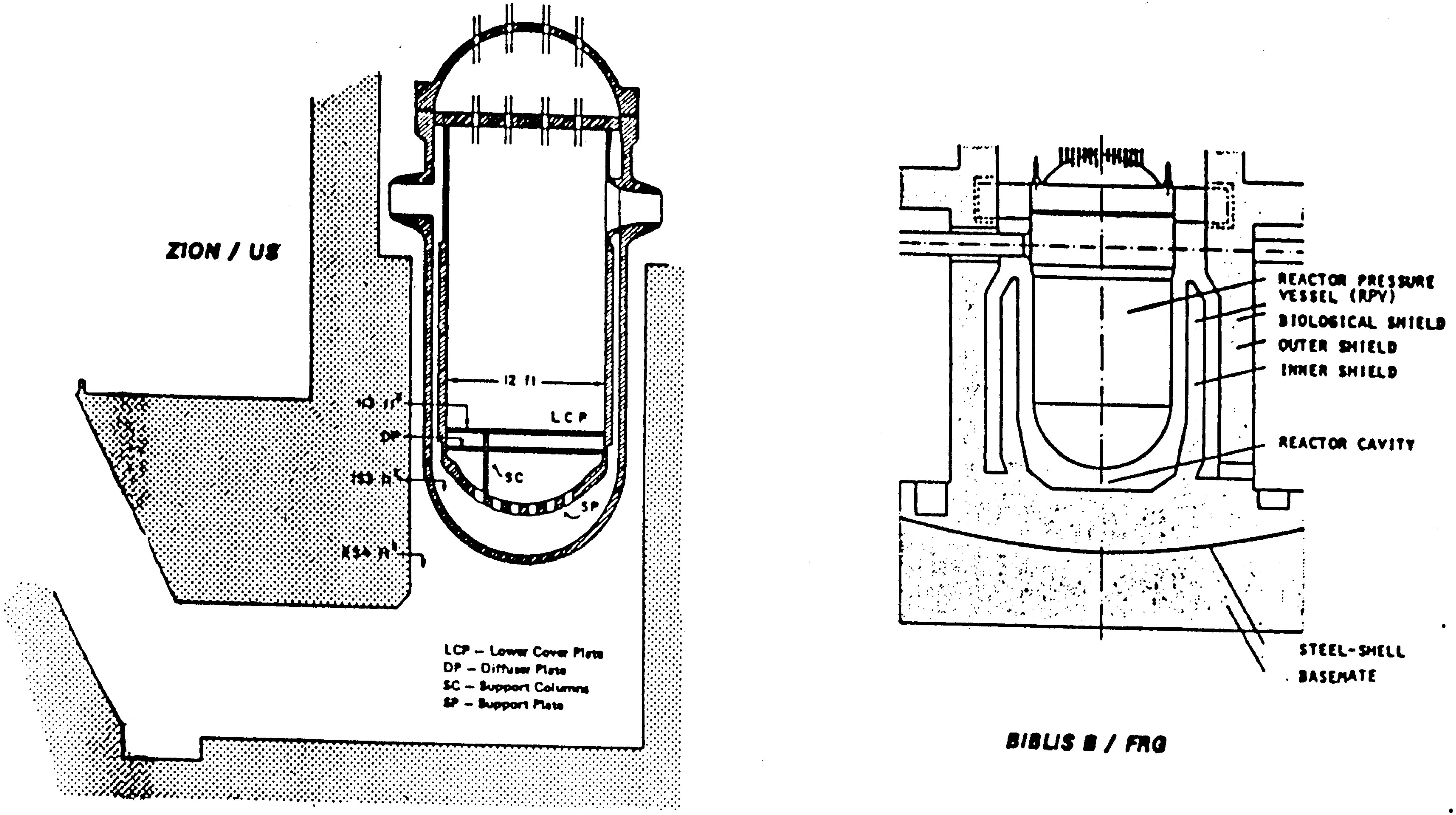


Fig. 13 : Different typs of reactor cavities

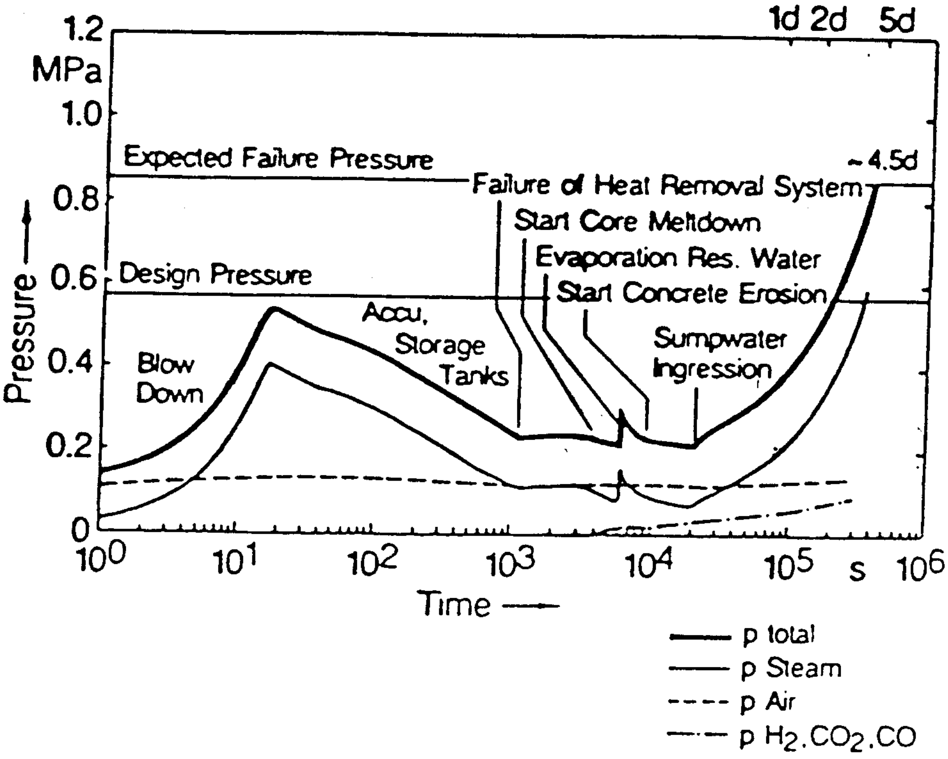


Fig.14 : Containment pressure-time history (Low-pressure case)

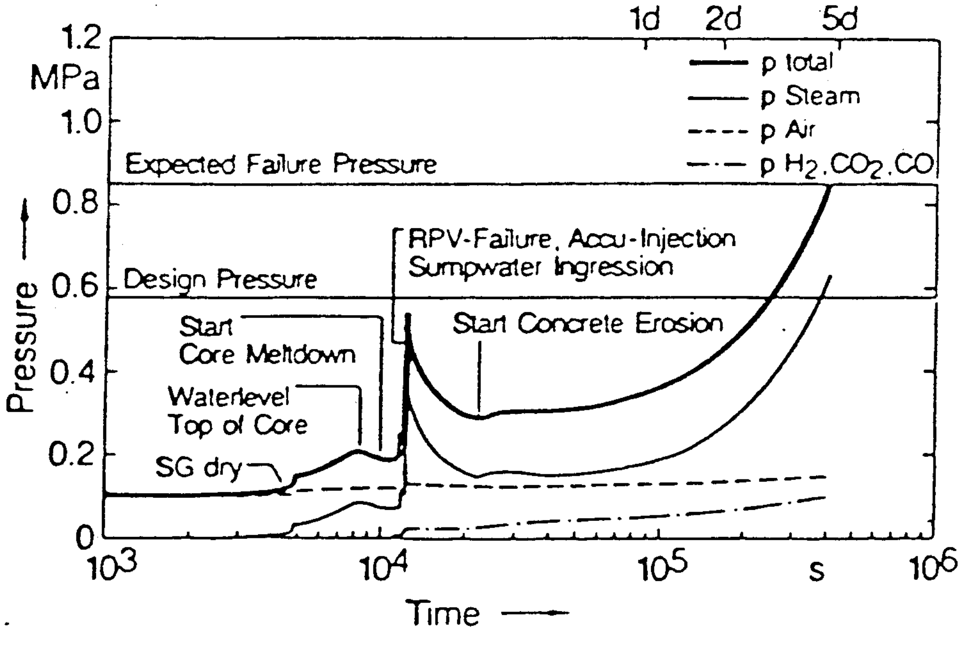


Fig. 15 : Containment pressure-time history (High-pressure case)