- the strategical aspect regarding the fissile material ressources, in expectation of the future introduction of fast breeder reactors.

The second point relates to safety, and in particular, to the safety image for the public. In the United States, studies have led to the notion of a "transparent" reactor, i.e. of a reactor with such a design that its high degree of safety can be easily demonstrated to the public. This has resulted in the notion of passive safety reactor, while that of an "intrinsically safe" reactor has been discarded. In this design, the forces of gravity and the stored energy are widely used (battery, pressure vessels) as well as natural convection. Obviously this limits power. Yet, it would allow "guaranteeing" the removal of residual power, thus avoiding the necessity of giving consideration to possible severe accidents - provided that reactivity accidents can be excluded and that the containment of radioactives products can be ensured.

Though the approach we have adopted is entirely different, some attention should be paid to the other studies undertaken about this concept for the following reasons:

- If the use of "passive" systems proves to be economic it can of high interest, provided that their reliability can be demonstrated.

- There might be an economic interest for reduced power reactors - a statement which remains to be confirmed - and in this case, the export commercial action should not be neglected ?

THE ROLE OF PASSIVE AND INHERENT SAFETY PROPERTIES IN SIEMENS/KWU NUCLEAR POWER PLANTS

O. GREMM
Siemens AG,
Unternehmensbereich Kraftwerk Union,
Erlangen, Federal Republic of Germany

Abstract

In Siemens/KWU Nuclear Power Plants the applied safety concept consist of a well balanced combination of active, passive use well is inherent safety measures.
In principle it is not possible to realise a safety concept exclusively with inherent and/or passive safety properties. The respective measures and arguments will be explained in detail in the presentation. In addition the Siemens/KWU safety concept with examples of the role of inherent and passive safety measures will be illustrated.

The safety philosophy of Siemens/KWU LWR is based on the principle of accident prevention by means of a defense in depth strategy using

- quality assurance in the broadest sense to reach good availability
  and
- designing the plants to withstand an all-embracing spectrum of design basis accident.

This is done in a multi-level concept of plant safety using active, passive and inherent safety measures.

With respect to the current discussion on new reactor concepts special inherent and passive safety features of Siemens/KWU design are explained in this paper.

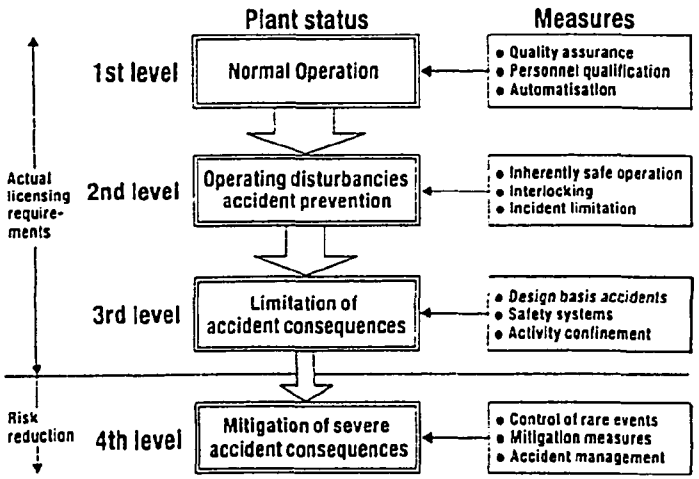

FIG. 1. Multilevel concept of LWR plant safety.

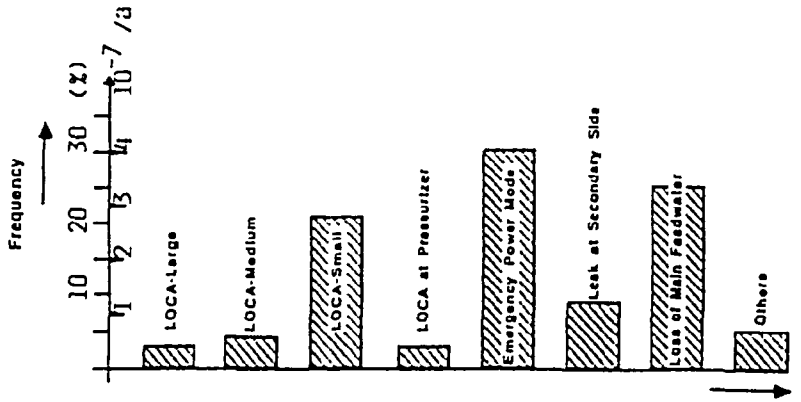

FIG. 2. Contribution to core melt frequency from different initiating events.

Stepwise improvement of the safety level of Siemens/KWU-LWR

Figure 2 shows the contributions of different initiating events to-the core melt frequency calculated for the Konvoi plants. The total core melt frequency is about 1.0 E-6 per annum as compared with the core melt frequency of approximately 1.0 E-4 per annum given in the German Risk Study Phase A for the reference plant Biblis B. The improvements result from

- Modifications in system technology,
- Feedback of experience,
- Results of safety research.

These improvements demonstrate the concern of Siemens/KWU for stepwise improvement of the safety of our plants in recent years.

Integrity of primary systems

We now consider steel pressure vessel technology for light water reactors to be fully mature. Putting into practice the quality requirements set out in the RSK Guidelines means that catastrophic failures can be ruled out. This also applies to other primary system components and particularly to the piping /2/. Catastrophic failure in this area is also ruled out by the quality control performed and the standard of quality achieved. The achieved quality means that the following safety characteristics of the passive pressure boundary exists as inherent features of the design:

- validity of the leak-before-break criterion,
- the quality status can be ascertained at all times.

Phase B of the German Risk Study containes realistic values for the frequency of occurrence of loss-of-coolant accidents, Fig. 3, /3/. Applied to Konvoi plants this means that LOCAs are only a minor contribution to risk. These new frequencies of occurrence have not yet been included in the data shown in Figure 2.

	DRS-A	DRS-B
LOCA large (> cm² 500)	$3 \cdot 10^{-4}$/a	$< 10^{-7}$/a
LOCA medium (cm² 80 -500)	$8 \cdot 10^{-4}$/a	-
" (cm²200 -500)	-	$< 10^{-7}$/a
" (cm² 80 -200)	-	$6 \cdot 10^{-6}$/a
LOCA small (cm² 2 -80)	$4 \cdot 10^{-3}$/a	-
(cm² 50 -80)	-	$4 \cdot 10^{-5}$/a
" (cm² 25 -50)	-	$3 \cdot 10^{-4}$/a
" (cm² 2 -25)	-	$4 \cdot 10^{-3}$/a

FIG. 3. Frequency of LOCA events (Biblis B).

In this connection I refer to the "working paper on Safety Related Terms" /9/. To my opinion on page 3 in the explanation of passive safety the word "design" should be added. Because passive safety rely not only on natural laws and properties of materials but also on the design of passive barriers. Therefore the complete explanation should be "... *passive safety means* that the reliance is instead placed only on natural laws, properties of materials and design of passive components and systems."

Realistic efficiencies for ECCS

In addition to the fact of lower frequency of LOCA events, results of recent research in connection with the efficiency of ECCS are of importance. The research during Phase B of German Risk Study shows that the active 4 x 50% systems are in most cases actually 4 x 100% systems /4/, Fig. 4.
This is an example how safety research has identified safety margins resulting in additional grace periods for secondary side cool down.

Containment Design

For KWU pressurized water reactors the reactor building consists essentially of the spherical steel containment vessel and the reinforced concrete outer shell surrounding it. The containment vessel for the 1300 PWR plant has a diameter of 56 m and acts after isolation as a passive pressure-tight and leak-tight con-

Leak cross section (sqcm)	System functions required					
	High pressure injections	Accumulator injections	Low pressure injections	Low pressure recirculations	Admissible delay of secondary side cool down (min)	Feedwater supplies
> 500	-	-	1	1	∞	
200-500	1	-	1	1	∞	
300-500	-	2	1	1	∞	
80-200	3 or 4	-	2	2	∞	1 main feedwater supply or 2 aux./emerg. feedwater supplies
	2	-	1	1	60	
	1	-	1	1	30	
50-80	2	-	1	1	60	
	1	3	1	1	60	
	1	-	1	1	30	
25-50	2	-	1	1	90	
	1	-	1	1	60	
2-25	1	-	1	1	> 120	
	-	-	1	1	30	

large leak
medium leak
small leak

FIG. 4. Minimal requirements for the system functions for emergency core cooling and residual heat removal in the case of leaks in a reactor coolant loop.

finement. This containment vessel is designed for the pressures and temperatures resulting from a design basis accident (complete break of reactor coolant line). Protection from external impacts is provided by the reinforced concrete shell.

The design pressure of the containment vessel (Figure 5) is calculated for a large-break LOCA under very pessimistic assumptions.

The design pressure is 6.3 bar, whereas under realistic assumptions, the accident pressure is only 4.2 bar (Figure 6). An additional safety margin comes from special design requirements of the steel sphere. Both resulting in an overall safety margin of nearly a factor of two which is important for the mitigation of core melt consequences.

- ☐ Design basis accident: Break of main coolant pipe
- ☐ Pressure build up by flashing inventory of the reactor coolant system and also that of the secondary side of one steam generator into the containment
- ☐ Decay heat: ANS standard + 20%
- ☐ Free volume of containment reduced by 2% Volume of primary circuit (+ steam generator) increased by 2%
- ☐ Design pressure = calculated pressure + 15% for safety
- ☐ Design pressure 6.3 bar at 145 °C, although wall temperature at maximum pressure only 60 °C
- ☐ A best estimate calculation results in a maximum pressure of 4.2 bar instead of 6.3 bar

FIG. 5. Thermodynamic design of the containment vessel.

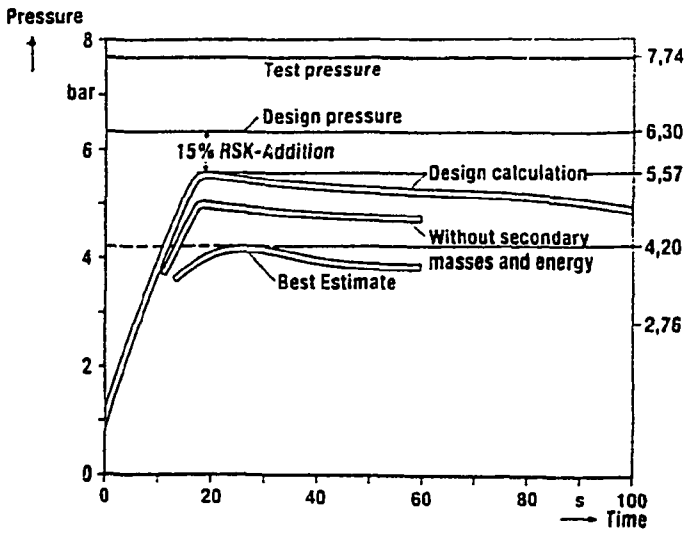

FIG. 6. Cumulative safety of pressure related design.

Reactivity Accidents, Reactor Protection

The fault-tolerant characteristics which assure reliable shutdown of light water reactors are based on inherent, passive and fail safe features (Figure 7).

Fault-tolerant technology:

- Actuation even on failure of 1st initiation
- Stored drive energy
  - . PWR: gravity
  - . BWR: accumulators

Inherent safety characteristics

- Self-regulation due to
  - . Negative void coefficient
  - . Negative coolant temperature coefficient
  - . Doppler coefficient
- ATWS controlled

Conclusion: No core degradation possible as a result of reactivity anomalies

FIG. 7. Fault tolerant and inherent shutdown characteristics.

The summary of the results of ATWS analyses given in /5/ demonstrating mitigation of these events as called for in the RSK Guidelines gives particularly impressive evidence of inherent characteristics (Fig. 8). These studies, in particular on older plants in which the borating system is not started automatically have shown, that the time available before manual or other active actions have to be taken, is approximately half an hour. For better understanding this fact, it should be referred to the first edition of RSK Guidelines 1974, were the requirement for ATWS investigation was included /6/.

	OPERATING TRANSIENT		Pressurizer solid after (s)	Maximum coolant pressure (bar)	Maximum coolant temperature (°C)	Maximum void content at RPV outlet (%)	Minimum DNB ratio	Maximum clad temperature
1.	Loss of main heat sink, e.g. due to loss of condenser vacuum or closure of main steam isolation valves with auxiliary power supply available		170	178	339	< 0	1.65	380
2	Loss of main heat sink with auxiliary power supply not available		27	188	355	8,0	< 1	520
3.	Maximum increase in steam extraction, e.g. due to opening of bypass station or of main steam safety valves		207	173	341	1,0	1,7	380
4.	Complete loss of feedwater supply		80	175	349	2,5	1,7	430
5.	Maximum reduction in coolant flow		90	178	342	1,0	1,7	450
6.	Maximum positive reactivity insertion due to withdrawal of control assemblies or control assembly groups starting at the operating conditions full load and at hot standby	Full load	--	161	328	< 0	1,4	480
		Standby	--	167	330	< 0	1,0	380
7.	Depressurization due to inadvertent opening of pressurizer safety valve		123	< 158	334	7,0	1,2	500
8.	Maximum reduction in reactor inlet temperature due to failure of an active component in the feedwater supply system		--	< 158	< 326	< 0	1,65	380

FIG. 8. Results of ATWS analyses, required by RSK Guidelines.

This example demonstrates how inherent safety features gives limitation of consequences in the short term phase of the event and grace period for active measures. But active measures are necessary to reach a stable situation. In addition to this inherent passive and fail safe characteristics Siemens/KWU plants are equiped with a hierarchy of

- automatic reactor control
- redundant limitation systems
- redundant reactor protection systems with diverse initiating criteria

In this connection a problem arises with the definition of "inherent" given in /9/: "... the plant will remain in the safe condition at all times". According to this definition, a negative temperature coefficient for reactivity, for example, would not fall into the inherent safety feature catagory because, for it to take effect the temperature has to rise, and this is a non-safety oriented change in system condition. This rise must be reversed again which works against the negative temperature coefficient so that a permanently safe condition cannot be reached.

Passive Residual Heat Removal

Except in the event of large-break and medium-break LOCAs which are purely hypothetical anyway as explained above, residual heat removal from the reactor core is performed in all design basis accidents by natural circulation in the reactor coolant system, with the heat passing across the heat transfer surfaces of the steam generators. This is demonstrated experimentally even in the presence of two phase flow and in the presence of inert gases.

This passive residual heat removal comes from the possibility of isolating the reactor coolant system in such a way that it acts as a passive barrier. In this context reference must be made to the reactor coolant pumps, which are provided with a so-called standstill seal, so that leakage from the reactor coolant system is so small, that no active systems for leakage make-up in the apparent in discussions on station black out:

- The steam generators are able to operate initially as heat sinks without active measures
- Subsequently the reactor coolant system can dissipate heat.

Thus giving grace period of 2 to 3 hours until core melt would start.

The absence of power supply is very often used as an argument in favour of passive systems. But this should not be overestimated, because this field is predestinated for the use of redundant and diverse measures. Siemens/KWU plants have

- connections to two independent grids
- the possibility of automatic changeover for houseload
- redundancy in emergency diesels

- a second diverse set of emergency diesels protected against external events
- additional connections to plants in the vicinity on most sites.

In KWU pressurized water reactors the frequency of loss of power is greatly reduced by the greater redundancy and diversity of the emergency power supply and also by the possibility of automatic changeover back to house load, which is not usually provided in reactor plants from other suppliers. If unavailability of the offsite grid, failure of the generator to supply house load power and also failure to start of the emergency diesels are postulated, no rapid actions are necessary, as explained above in connection with station black out.

Testability, Reparability and Inservice Inspection of active and passive Systems

Safety systems can be tested nearly completely during plant operation. This is of great influence on the availability in case of a demand. A major planning and layout principle in KWU reactors is the complete reparability and inspectability of the plants. This principle has proven extremely useful especially with respect to the prevention of failures at passive components. Implementation gives rise to the following inherent characteristics:

The quality status of the plant can be

- established
- maintained at constant levels or
- even improved.

The last-named applies in particular to the overcoming of possible teething trouble, a problem which a responsible manufacturer should not rule out in newly developed plants. Therefore good reparability and examinability must be required in particular in plants which are based on novel principles.

Availability Redundancies

The primary and secondary side operational systems are provided with availability redundancies. Therefore the plant normally remains in operation in the case of a component failure. Simultaneously this results in a lower frequency of demands of the safety systems (Fig. 9).

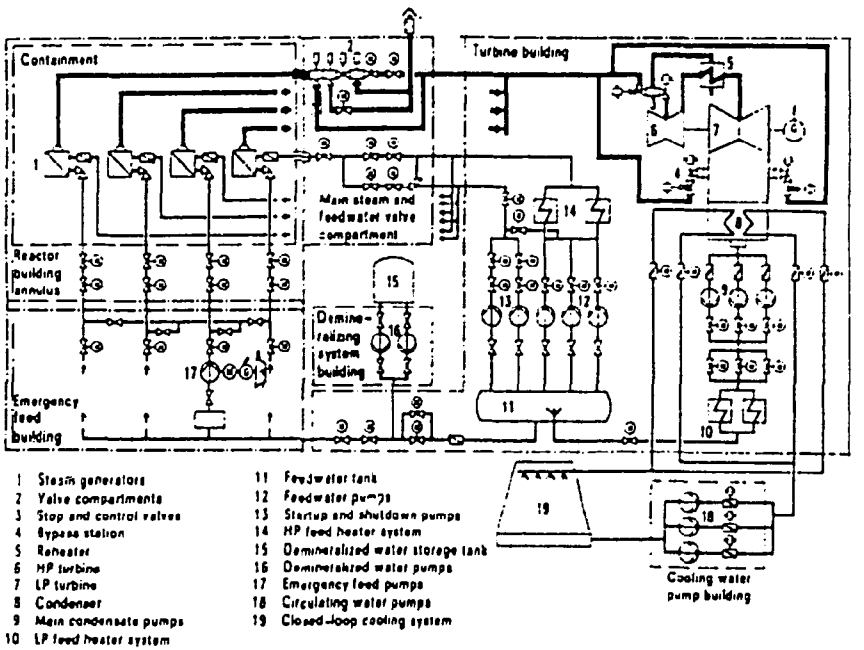

FIG. 9. 1300 MW PWR secondary-side heat removal systems.

This means simultaniously less frequent impact on the passive primary system barriers. With this respect we have to keep in mind, that pressure and temperature variations resulting from transients give active impacts on the above mentioned barriers.

In this respect I would like to make a second proposal for the definitions and explanations in /9/ with respect to passive safety which is of special importance for passive barriers. The design has to include active impacts like, loads, variation of loads, corrosion and may be other problems.

Accident Management

The Safety margins which are partly explained in this paper are important and effective for mitigation of severe accidents and give ample time for accident management measures /7, 8/.

Conclusions

Siemens/KWU-PWR have reached a safety level which is satisfactorily and can do the further development in an evolutionary way and especially using the knowledge modules explained on this paper. Doing it this way means, that the experience of more than 200 LWR plants can be used in the future. This is of importance because no other reactor system has been investigated in such depth with reagard to safety considerations.

REFERENCES

/1/ W. Bürkle, W. Braun
Inherent Safety Features of Advances Light Water Reactors
Proc. of an IAEA Conference on Nuclear Power Performance and Safety, Vienna, 28. Sept. - 2 Oct. 1987

/2/ RSK Guidelines for Pressurized Water Reactors, 3rd Ed 1981, Editor: Gesellschaft für Reaktorsicherheit, Cologne.

/3/ F. Heuser
Specialist Meeting of the Gesellschaft für Reaktorsicherheit,
Cologne, November 12 to 13, 1986

/4/ H. Hörtner, German Risk Study, Phase B, Results of the Event Tree and Fault Tree Analysis,
International Topical Conference on Probabilistic Safety Assessment and Risk Management,
Zürich, Aug. 30 - Sept. 4, 1987 p. 419

/5/ Volume 10, PWR in "Handbuchreihe Energie" Section 3.10, Operational and Accident Behaviour
G. Frei et al, to be published

/6/ see /2/ first edition from 1974

/7/ K. Geyer, O. Gremm, U. Krugmann, R. Roth-Seefrid,
Accident Management Measures for KWU Nuclear Power Plants,
Kerntechnik 50 (1987) No. 2 p. 86

/8/ J. Czech, U. Krugmann,
Accident Management Procedures for Siemens AG KWU Group Pressurized Water Reactors,
Proc. of the ENS/ANS Conference on thermal reactor safety, NUCSAFE '88, 2.-7. Oct. 88, Avignon, France

/9/ Description of Safety Related Terms,
Working Paper on Safety Related Terms, established during Consultants Meeting on Description of Passive Safety Related Terms, Vienna, October 3rd, 1988.