IAEA-TECDOC-861

Review of design approaches of advanced pressurized LWRs

Report of a Technical Committee meeting and Workshop held in Moscow, Russian Federation, 10–13 May 1994

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

January 1996

The IAEA does not normally maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,— in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.

The originating Section of this publication in the IAEA was:

Nuclear Power Technology Development Section
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

REVIEW OF DESIGN APPROACHES OF ADVANCED PRESSURIZED LWRs
IAEA, VIENNA, 1996
IAEA-TECDOC-861
ISSN 1011-4289

Printed by the IAEA in Austria
January 1996

FOREWORD

This TECDOC presents the results of a comparative review of design approaches of advanced pressurised light water-cooled reactor designs, consisting of contributions from different vendors and organisations with reference information on their advanced PWR designs, and conclusions from the IAEA Technical Committee Meeting and Workshop that was convened in Moscow, Russia, from 10 to 13 May 1994.

This comparative review has been carried out within the IAEA's Nuclear Power Programme in the frame of activities recommended by the IAEA International Working Group on Advanced Technologies for Water Cooled Reactors.

In the early stages of preparations for this meeting, it had been concluded that - for the plant designs to be reviewed - general technical descriptions, of adequate detail, could mostly be found in the literature, and that this review should focus on a set of characteristic features, or safety functions, rather than repeating well-known material. To this end, a rather detailed format for written information on the different designs was prepared, and sent out to the vendors or design organisations, together with an example of a completed design description.

Most of the vendors or design organisations described their design approach in accordance with the specified format, which consists of a brief description of the plant design and its safety philosophy, descriptions on how certain safety functions are accommodated, and a data list. Based on these contributions, the measures incorporated into the designs to accomplish the selected safety functions can be easily reviewed, discussed, and compared.

The Technical Committee Meeting and Workshop was devoted to review and discuss differences and commonalities in the various design approaches with the aim of increasing the understanding of the design decisions taken, and a number of general conclusions were drawn. Though many differences in design approaches were found in the presentations, a number of common features could also be identified. These included design approaches to achieve further improvements with respect to safety, design simplification, reduction in cost, incorporation of feedback from operating experience, and control room improvements regarding human factors and digitization. Design approaches to achieve further improvements in safety included consideration of severe accidents in the design process, increased thermal margins and water inventories, longer grace periods and double containments.

Several suggestions for further activities were made at the Workshop, primarily "cross-cutting studies" on the basis of the information presented at the Technical Committee Meeting that go into greater detail as to how the different designs or design concepts differ in the 15 key design areas addressed in the papers.

The IAEA wishes to express its appreciation of the work done by all parties that have contributed to this effort.

EDITORIAL NOTE

In preparing this publication for press, staff of the IAEA have made up the pages from the original manuscripts as submitted by the authors. The views expressed do not necessarily reflect those of the governments of the nominating Member States or of the nominating organizations.

Throughout the text names of Member States are retained as they were when the text was compiled.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights.

CONTENTS

Part I
RESULTS OF THE TCM AND WORKSHOP

1. INTRODUCTION

1.1. Background and purpose of the TCM

In many countries with a civilian nuclear power programme significant efforts are under way to develop and design advanced and improved versions of the currently operating nuclear power plants that form the base of experience. The objectives for improvements cover a broad range of interest such as minimizing risk, gaining better economics, improving reliability and enhancing safety. Most of the reactor concepts being developed are evolutionary, but some developmental concepts, incorporating varying degrees of innovation, are also being proposed. These concepts are of course in different stages of development, design, and licensing.

Many development activities in Western countries either have already reached, or are close to reaching important milestones, such as establishing utilities' requirements, submitting plant designs for regulatory approval, or receiving regulatory approval. There are some new Russian reactor designs also with features the discussion of which would be mutually beneficial.

In view of these circumstances an IAEA Consultancy in September 1992 recommended pursuing a Russian initiative for reviewing design approaches and safety features of various reactor concepts. The initiative consisted of compiling a consistent set of characteristic features of the Advanced Reactors, followed by their discussion at a Technical Committee Meeting and a Workshop. The scope of these activities was limited to pressurized light water reactors. The purpose was to discuss the measures considered in the designs for a limited number of safety features in order to increase the mutual understanding of the design decisions taken. Of great importance in this context are also the applicable codes, standards and national safety requirements on which the different designs are based.

1.2. Approach

To this end a special approach was taken in which the authors of the contributions in the TECDOC were asked to prepare their material in a relatively rigid format consisting of three parts. The first part of each paper gives an overview of the respective plant or plant concept, emphasizing the rationale for the selected technical approach. The second part consists of a description of the solutions employed in 15 key design areas. All concepts had to specifically address these design areas which, for reference, were taken from that part of INSAG-3[1)] that deals with plant design. The third part of each paper is a listing of important design parameters. The main body of the TECDOC is thus structured as shown in Table 1.

INSAG-3 is a widely accepted internationally developed recommendation of principles that, if properly followed and implemented in the design of a nuclear power plant, would assure a very high degree of safety. As the practice in many countries either follows directly the approach practiced in the USA, or is to a large extent based on the latter, a juxtaposition of the key topics addressed in INSAG-3 and their correspondence in Regulatory Guide 1.70 of the U.S. NRC was prepared by one of the organizations contributing to this TECDOC in order to facilitate the desired better understanding of various design approaches. Since this

[1)] *Basic Safety Principles for Nuclear Power Plants, Safety Series No. 75-INSAG-3, IAEA, Vienna 1988.*

TABLE 1. STRUCTURE OF PAPERS CONTAINED IN THE MAIN BODY OF THIS TECDOC

1. General description of plant or plant concept
2. Specific design features as referenced in INSAG-3
    1. Plant process control systems
    2. Automatic safety systems
    3. Protection against power transient accidents
    4. Reactor core integrity
    5. Automatic shutdown systems
    6. Normal heat removal
    7. Emergency heat removal
    8. Reactor coolant system integrity
    9. Confinement of radioactive material
    10. Protection of confinement structure
    11. Monitoring of plant safety status
    12. Preservation of control capability
    13. Station blackout
    14. Control of accidents within the design basis
    15. Mitigation and control of severe accidents (not explicitly addressed in INSAG-3)
3. Key design parameters

comparison is generally design independent it is placed before that part of the TECDOC that contains the individual plant descriptions. Most of these plant descriptions were made available to the participants of the TCM and the Workshop prior to the meeting in Moscow.

Conduct of the TCM and Workshop

The Technical Committee Meeting, organized in Moscow from 10 to 13 May 1994 had the objective of identifying trends in the development of Advanced Pressurized LWRs in different IAEA Member States. The plant concepts presented are shown in Table 2.

The TCM was organized into three consecutive sessions. The first two dealt with Large-Size and Medium-Size plants, respectively. The third session covered other items of the meeting, specially, "Development of containment concepts", "Reactor core design and I&C for Temelin NPP" and "Safeguards aspects in the design of NPPs".

The presentations during the first two sessions emphasized those features that are in the view of the individual designer of greatest importance for meeting the recommendations laid out in INSAG-3, and as described in the main papers. Such a condensed survey, summarizing the main design solutions in the field of plant safety, and some characteristics and technical data of the plants reviewed, should help to enable identifying the trends in enhancing safety and plant reliability. Commonalities and differences in the approaches leading to an enhancement of safety and reliability were also sought and briefly identified. They formed the lead-in to the subsequent workshop at which both objectives and technical solutions were discussed in greater detail.

TABLE 2. DESCRIPTIONS PREPARED FOR TCM
(in the order presented)

	Name of NPP	Country	Design Organization
Large-size NPPs			
1.	VVER-1000 (V-392)	Russia	Gidropress
2.	System 80+	USA	ABB CE
3.	Sizewell B	UK/USA	Nuclear Electric/NCC/ Westinghouse
4.	Convoy	Germany	Siemens
5.	N4	France	EdF/Framatome
6.	EPR	France/Germany	NPI
Medium-size NPPs			
7.	AP-600	USA	Westinghouse
8.	VVER-500/600(V-407)	Russia	Gidropress
9.	VPBER-600	Russia	OKBM
10.	PIUS	Sweden	ABB Atom
Other concepts			
11.*	AC-600	China	CNNC
12.*	MS-600	Japan	NUPEC
13.*	APWR	Japan/USA	NUPEC/Mitsubishi/ Westinghouse

* These concepts were neither presented nor discussed at the TCM. The prepared material is retained in Appendix I for completeness.

Scientific visits to the Russian Research Center Kurchatov Institute in Moscow and to the Experimental Design Organization Gidropress in Podolsk took place for the purpose of the participants having intensive exchanges on their experience and actual development work.

Thirty representatives mainly from designers and developers of advanced LWRs came from 10 different countries. There were three IAEA representatives from Vienna. The list of participants is given in Appendix II.

The TCM and the Workshop were organized by the IAEA in the framework of the International Working Group on Advanced Technologies for Water-cooled Reactors (IWGATWR) and were hosted by the Kurchatov Institute in Moscow, Russian Federation. The meetings were chaired by Mr. Ponomarev-Stepnoi, Deputy Director of the Kurchatov Institute. The sessions of the TCM and the Workshop were chaired by Mr. Gagarinski with the assistance of Messrs. Ritterbusch and Gherardi. The scientific secretaries of the IAEA were Messrs. Krett and Goetzmann. Messrs. Novikov and Ignatiev served as scientific secretaries from the host organization. The meeting was opened and closed by Mr. Ponomarev-Stepnoi of the Kurchatov Institute together with Mr. Kupitz of the IAEA.

2. SUMMARY OF THE TCM

This section of the report highlights the various plant designs presented at the TCM and described in the main part of this TECDOC. The ordering is in accordance with the agenda adopted for the meeting. The technical descriptions are preceded by a summary of two presentations on the framework within which ALWR development takes place in the Russian Federation (RF), and in the United States (US), respectively, since in these two countries a number of different LWR concepts are being developed more or less simultaneously. These presentations were given by Messrs. Kukharkin and Lang.

2.1. Light Water Reactor Development in the Russia and in the USA

The development of nuclear power in Russia started in 1954, when the first NPP was put into operation in Obninsk. The technical foundation for this development were vessel-type plutonium reactors. In the ex-USSR the growth rate of nuclear power was 4-5 GWe/year; the total power of all the NPP amounts to 36 GWe in early 1994; the existing fuel cycle capacity can serve up to 100 GWe. The situation in Russia is shown in Table 3.

TABLE 3. NPP TYPES AND CAPACITY IN RUSSIA

	TOTAL	VVER	RBMK	FAST REACTORS	EGP*
Number of NPP	9	4	3	1	1
Number of units	29	13	11	1	4
Tot. power, MWe	21242	9594	11000	600	48

* Bilibino Nuclear Power Station

Three generations of LWR have been developed in Russia. These are VVERs with an electric power output between 440 and 1000 MW per unit. The safety level of the operating NPPs, considering the planned measures, meets in principle the international requirements for existing NPPs.

Currently a new generation of LWR is being developed in Russia, named VVER-1000, VVER-500, and VPBER-600. Their key features are passive protection, improved inherent safety and stability in case of severe accidents, and improved economic and operational indices. The concept for deployment of nuclear power in the Russian Federation approved in 1992 proposes an increase of the total power of all operating stations from 30 to 38 GWe until 2010. Along with the NPP with VVER, the development of NPP for district heating, and advanced channel reactors is also planned in Russia.

In conclusion it can be said that most of the operating VVER reactors meet international safety requirements. The VVER-440 of the first generation, although having some deviations from current safety standards, possesses a high degree of inherent safety. It is hoped that its safety will be proven in terms of PSA with the consideration of "leak-before-break" concept and with some backfitting measures. Beyond that, Russia has a number of new generation NPP designs under development. Their safety in terms of PSA is by two and more orders of magnitude higher than that of the operating NPPs.

The ALWR programme in the USA comprises in scope the following three items. The first one is the design certification of the evolutionary plants ABWR of General Electric and System 80+ of ABB Combustion Engineering. Design development and design certification of the simplified passive plants SBWR of General Electric and AP-600 of Westinghouse is the second item. First-of-a-kind engineering (FOAKE) to achieve commercial standardization for the ABWR and the AP-600 comprises the third task.

Funding of most of the above activities is shared between the Department of Energy, the reactor vendors, the Electric Power Research Institute, and in the case of FOAKE, 15 utilities from the U.S. Important milestones are shown in Table 4.

TABLE 4. IMPORTANT MILESTONES OF THE U.S. ALWR PROGRAMME

	ABWR	System 80+	AP-600	SBWR
Final Safety Evaluation Report	7/94	7/94	~8/96	~3/97
Final Design Approval	7/94	7/94	~9/96	~6/97
First-of-a-Kind Engineering	9/96	-	9/96	-

For each project, formal design certification is expected to follow Final Design Approval by 15-18 months. The schedules for the passive plants are dependent on the timely and successful completion of various testing programmes, many of which are being conducted outside the United States.

2.2. Key features of large-size NPPs

VVER-1000 (V-392) Advanced Reactor Plant (B. Volkov)

With a thermal power of 3000 MW the V-392 represents the latest version of the VVER-1000 reactor line. The design is developed in accordance with the latest version of the RF Safety Regulations. IAEA QA requirements and International Standards ISO 9000 are also taken into account in the design. The principal design features of VVER-1000 are:

- 4-train RCS with horizontal steam generators with large water inventory,
- Subcriticality provision with control rods at any moment of the lifetime, considering a coolant temperature decrease to 120°C,
- quick boron supply system,
- automatic control system of improved reliability with self-diagnosis and expert system giving advice to the operator,
- system of passive residual heat removal in case of a station blackout and loss of emergency power supplies for 24 hours,

- core passive flooding system designed to remove residual heat during the last stage of a LOCA for not less than 12 hours,
- filtered double concrete containment

System 80+ (S. Ritterbusch)

System 80+ was recently approved by U.S. Regulators. In the design process, emphasis was placed on improved safety and severe accident design features. Also stressed were improved accident prevention through "Defense-in-Depth" by increasing margins and adding equipment. For example, major System 80+ features are :

- larger steam generators and pressurizer and improved materials,
- lower operating temperature and more thermal margin,
- new, all-digital control room,
- larger containment with hydrogen igniters,
- safety-depressurization system with in-containment water storage tank,
- gas-turbine generator as diverse source of electrical power,
- large reactor cavity floor with cavity flooding system,
- increased earthquake design and seismic margins.

As a result of these measures, safety is improved by a factor of 100, and technical justification for simplified emergency planning has been established.

In the context of the present meeting it should be noted that the USA has developed and approved standardized approaches to severe accident treatment (eg., U.S. NRC report SECY-93-087 and EPRI Utility Requirements Document).

Sizewell B (J. Bartlett)

The design of Sizewell B was determined inter alia by the objective that doses and accident frequencies/consequences must be kept as low as reasonably practicable (ALARP). This is a fundamental requirement, and is the basis for the design and safety principles for nuclear power plants in the UK. Following the TOR document (The Tolerability of Risk from Nuclear Power Plants, HMSO - 1992), probabilistic analyses have become an important tool for selecting "design measures" complementing the deterministic design base. There are four (instead of two or three) levels for correlating doses with frequencies.

Important design features of the Sizewell B plant include:

- 4-train systems organization
- 30 minutes tolerance before operator action
- fully computerized reactor protection system
- station blackout addressed by two reliable grids and four emergency diesels
- corium retaining basemat.
- filtered secondary containment.

Convoy (J. Czech)

In the design key emphasis was placed on accident prevention. A limitation system, structured in analogy to the reactor protection system, serves as a means to reduce the need (frequency) for actuating the safety systems. Other important features include:

- high degree of automation to cope with human errors,
- single failure and "repair" leads to 4 x 50%, in some cases to 4 x 100% redundancies,
- strict separation of redundancies with no cross-connections,
- 4 large diesels for "normal" events plus 4 small diesels for external events, the latter to be used also for station blackout,
- protection against military aircraft crash,
- double containment with annulus exhaust filtration.

The three-level defense in depth concept is expanded by a fourth level addressing mitigation of core melt consequences by accident management procedures.

N4 (J.P. Berger)

The N4 design takes credit of lessons learnt from experience. The safety approach is deterministic (needed for the practical design), complemented by probabilistic analyses to get design homogeneity. The classical defense-in-depth is expanded by a fourth level addressing accident management. The safety improvements lead:

- from event orientation to state orientation to arrive at improved emergency procedures;
- to design changes and equipment additions, e.g.:
    - more accurate and functionally adapted instrumentation,
    - means to deal with total loss of frequently used systems,
    - implementation of control systems and procedures to deal with shutdown operating conditions.

Other important features of N4 are:

- a computerized control room with a classical auxiliary "panel" as a back-up,
- mitigation of core melt in ultimate conditions, with filtered venting.

EPR (M. Yvon)

The EPR design draws upon both French and German experience. The approach to safety is deterministic, complemented by probabilistic considerations. The latter contains as a "new" element the concept of risk reduction with the two objectives of limiting the integral frequencies (a) for core damage to 10^{-5} per reactor-year and (b) for a large release to 10^{-6} per reactor-year. At the present early design stage, design targets are specified to be about 10 times lower regarding internal events. For public protection in case of severe accidents the following objectives were formulated:

- no stringent countermeasures to be taken before 24 hours,
- no need for evacuation or relocation beyond the immediate vicinity of the plant (few

kilometers),

- no foodstuff restriction beyond 1 harvest.

Important design features of the EPR are:

- 4-train systems configuration,
- protection against military aircraft crash,
- elimination of high pressure core melt by design measures,
- containment design against low pressure core melt consequences, e.g. containment bypass and early failure eliminated by design measures,
- "dry" corium spreading,
- strong - 7.5 bar - containment to have margins and no need for early heat removal from the containment.

2.3. Key features of medium-size NPPs

VVER-500/600 (V-407) Advanced Reactor Plant (B. Volkov)

The estimated probability of the design limits being exceeded must be less than 10^{-5} per reactor-year. The estimated probability of considerable fuel damage leading to the necessity of a population evacuation should be less than 10^{-7} per reactor-year. These goals are achieved by consistent implementation of the defense-in-depth principle based on a broad utilization of passive safety systems.

Important design features are:

- low specific fuel power;
- reactor subcriticality to be achieved with control/shutdown rods for coolant temperatures down to 100°C;
- reduced number of pumps, compressors, valves, penetrations, etc;
- passive emergency core cooling system;
- systems of passive heat removal from the reactor and from the containment;
- 2 diesel generators.

VPBER-600 (V. Kuul)

The design relies upon the use of an integral reactor placed in a guard vessel. Intrinsic self-protection properties, and passive safety systems devices limit unfavorable consequences of failures in the external systems, loss of power, plant personnel errors and of subversive actions.

The reactor self-protection features comprise:

- elimination of large diameter primary-coolant pipelines;
- large volume of coolant above the core;
- high degree of primary coolant natural convection providing effective emergency residual heat removal;
- reduced neutron fluence to the reactor pressure vessel;
- a passive emergency residual heat removal (ERHR) system providing reactor cooling

for at least 3 days; this system does not depend on the steam generators and secondary circuit equipment and pipelines;

- a guard vessel providing the capability to keep the core covered with coolant and the capability to cool the reactor down; in addition, the guard vessel provides reliable confinement of radioactive products after loss-of-coolant accidents.

The capability to confine corium inside the reactor vessel or in the guard vessel is being validated in the design for the postulated accident with a reactor core melt, taking into account the specific features of the plant. This capability is characterized by an effective convection of the steam/water mixture inside the RPV, by a reduced heat load to the RPV, and by an adequate heat transfer from the outer surface of the RPV to the high-pressure atmosphere in the guard vessel. Further heat removal is effected via the emergency heat removal system.

AP-600 (E. Mink)

The approach to safety is characterized as follows. Non-safety grade systems are able to cope with the majority of design basis events, but passive, safety-grade features provide the ultimate protection. The provision of ample thermal margins is emphasized in the design.

No operator action is needed for the first 36 hours in the course of design basis events, although some very low probability accidents may make it desirable that operator action takes place sooner.

Key features/properties of the passive system(s) are:

- transients and leaks up to 6" equivalent diameter can be handled without system depressurization;
- automatic depressurization is needed for mid-size leaks (if charging pumps are not available);
- the highest peak cladding temperatures occur in the course of a large pipe break (1800 deg F (982°C), evaluated with conservative assumptions);
- heat removal from the containment is accomplished by a combination of wetting the outer containment surface and natural circulation of air through the annulus between the shield building and containment.

The selected design approach, in addition to enhancing overall safety, provides higher availability, plant simplification, reduced cost, and shorter construction schedule.

PIUS (T. Pedersen)

PIUS builds on established LWR technology, basically a reconfigured PWR, with the core portion of the primary loop enclosed by a large pool of borated water, and with permanent openings between the primary loop and the pool. The pool is contained in a large prestressed concrete structure constituting the lower portion of the pressure vessel. The primary circuit is a 4-loop arrangement with once-through steam generators and glandless pumps. The whole nuclear steam supply system is enclosed in a concrete containment; the reactor building serves as secondary containment.

Coolant circulation through the core is always in natural mode. The speed of reactor coolant pumps is controlled to achieve a pressure balance in the opening below the core; the pressure balance in the upper openings is accomplished by volume control. There are no control rods; power is controlled by adjusting boron content (slow), and by variation of coolant temperature (rapid) using secondary side heat removal control.

Major disturbances result in pool water ingress, shutdown and heat transfer to the pool. From the pool, heat is dissipated to ambient air in natural circulation via submerged heat exchangers in the pool and air cooling towers on top of the building. During normal operation pool cooling is active.

Reactor protection system, reactor scram system, and other traditional safety systems are provided, but they are not essential for core damage prevention.

The traditional spectrum of Design Basis Events has been analyzed assuming single failure, no operator action, ATWS and failure of all active systems. No accident sequence leading to core damage has been identified. Super-conservative PSA has given a core damage frequency well below 10^{-7} per reactor-year.

2.4. Other topics

The following three presentations address some specific technical aspects that can have a bearing on the design of future NPPs. Although they do not fit the scope of a full plant description, they are retained in this TECDOC for reference purpose.

Swiss Activities on the Development of Containment Protection Features in Case of Severe Accidents and the Experimental Investigation of Long-term Passive Decay Heat Removal Systems (T. Bandurski).

The motivation for the work is the evolving shift from "design basis accident concept" to "design basis accident and core meltdown accommodation" in order to be able to reduce emergency planning provisions. In this context three complements are being looked at: filtered venting, a core catcher concept and H_2- mitigation. The advantages of filtered containment venting with a three stage filter and water scrubber are: proven technology, corrosion resistance, resistance to clogging and easy to clean. The core catcher concept ACCIS (anti-corium-concrete-interaction-system) is a coolable, initially dry crucible that contains the corium thanks to the HIP-BN (high isostatic pressurizing boron nitride) material properties: melting point 3000°C, high thermal conductivity and thermal shock resistance. H_2-mitigation is based on a venting strategy (steam inertization) together with catalytic recombining. Its advantages are: passive system, H_2-removal under high steam concentration, and increasing effectiveness with increasing temperature.

The ALPHA-project relates to the investigation of passive decay heat removal, and fission product retention in ALWRs, and the related code development. The PANDA facility simulates a large scale integral containment system. In the LINX project large scale mixing and condensation phenomena are investigated to study the characteristics of possible internal building condensers under forced convection flow in the presence of non-condensible gases. Aerosol retention is investigated in the AIDA facility.

Instrumentation and Control Upgrade for the Temelin NPP (P. Tomanek)

The NPP Temelin in the Czech Republic is similar to other plants of the VVER-1000 type. The basic reason for the change of the I&C system is to enhance the safety and reliability of the NPP within its original conception and layout. After a review of the I&C system for the Temelin plant by foreign experts it was decided to upgrade the I&C system with the installation of Westinghouse technology. The preliminary design and replacement study was performed by ABB and Westinghouse.

The modern digital I&C system is based on microprocessor technology with multiplexing of information and control signals within a redundant and diversified structure. The I&C system covers: reactor protection system; reactor control system; diverse protection system; plant control system; unit information system. The diverse protection system is a safety system that protects the Temelin plant from a postulated common mode failure in the reactor protection system. The technology (hardware and software) is diverse from the reactor protection system and is configured in three trains.

Aspects of Agency Safeguards in Nuclear Plant Design (R. Fagerholm)

In order to comply with IAEA safeguards agreements negotiated with a State, the plant design should enable the establishment and maintenance of a system of accounting for, and control of all nuclear material passing through, or residing in the facility. The design should allow for the Agency's verification which includes, inter alia, independent measurements and observations conducted by the IAEA in accordance with specified procedures.

NPT safeguards agreements allow for the IAEA to arrange to use its own equipment for independent measurements and surveillance, and to arrange to install such equipment and to apply seals and other identifying and tamper-indicating devices to containment structures. Similar arrangements are also possible under other types of agreements. The precise manner in which this equipment is to be installed is decided through discussions between the State, the operator of the plant and the IAEA. Clearly, if the need for such safeguards measures is recognized in the original design of the facility, including relevant equipment, this could greatly assist the implementation of such measures.

In a decision taken by the IAEA Board of Governors in 1992, it is recommended that parties to comprehensive safeguards agreements should provide design information to the Agency at the time of the decision to construct (well before construction actually begins) any nuclear facility in order to, inter alia, facilitate the incorporation into the facility design of features which will make it easier to implement safeguards at the facility including the installation of safeguards equipment during construction of the facility.

Current internal IAEA discussions are focussing on the possibilities to produce plant-type specific guidelines concerning design-related safeguards aspects. These discussions may be extended to involve Member States experts in 1995/96.

3. SUMMARY OF THE WORKSHOP

3.1. Purpose and scope of the workshop

The key purpose of the Workshop was to identify and understand the commonalities and differences in design approaches followed in different countries. To this end the Workshop was conducted in two parts. During the first one presentations were made, mostly by representatives from Russian organizations, reflecting the approaches described in the working material for the TCM, but dealing also with new information and discussion points presented and raised at the TCM. The second part of the Workshop consisted of a more general discussion about the key approaches for assuring safety and in what context they have to be seen, and about how these approaches could be presented in a most concise way. Finally, it was observed, and briefly discussed, that there are still inadequacies in the precise understanding with respect to both certain physical phenomena, mostly in the area of severe accidents, and to how they are being addressed in the countries represented at the TCM. The following sections summarize the main points made during the two sessions of the Workshop. The related conclusions will be presented under a separate section. The two sessions of the workshop were held in full plenum since the question of design approaches was of basic interest to all of the participants.

3.2. Emphasis of ALWR development in Russia

From the preceding presentations Mr. Kukharkin drew the observation that core damage prevention and severe accident mitigation are the most important topics for coming to a full common understanding. The question was asked whether high core power densities which are desirable for economic reasons would have to be limited in order to ease the task of assuring adequate safety as may be concluded from looking at the different designs. It was also observed that there are differences in the postulates regarding core melt accidents and in the approaches how to deal with them. It seems that in the reviewed designs not enough attention is being given to this aspect because the emphasis is on prevention. As far as Russia is concerned, consideration of core melting is required, including steps to prevent progression to worse situations. The question was raised whether this is true for other countries as well, and if so, with what type of containment (e.g. different types of containments with or without filtered venting systems).

The main goal of the Russian programme RASPLAV is to study physical and chemical properties of corium and the processes of core melt-vessel interaction. It is very important to comprehend the possibility of heat removal from the external surface of the reactor pressure vessel (RPV), including flooding the reactor cavity with water, or use of the guard vessel (VPBER).

Another feature is the utilization of passive systems for ultimate heat dissipation to the environment. The speaker was concerned that some projects seem to reject the utilization of passive features. Mr. Kukharkin observed that increased automation and digitization of control, as it is the trend in western countries, are correct approaches and that great progress is being made in Russia in these areas, partly by drawing on the experience made in the West, and partly through a better understanding of severe accident dynamics. In closing, he also agreed with the targets of keeping large release frequencies in the range of 10^{-6} to 10^{-7} per reactor-year, but he also stated that the frequencies of large releases due to external events may be much higher. Finally, he observed that there are still differences concerning exposure limits, exclusion zones and emergency planning, specifically evacuation, all related to large releases.

3.3. Commonalities and differences in design approaches

A first attempt at identifying commonalities and differences in design approaches was made by several Russian experts. Mr. Novikov observed that all design approaches seem to meet accepted principles even though significant differences do exist. These differences seem to be larger between mid-sized and full-sized reactors as a group each, than between the concepts within either group (Figure 1). This more general observation was extended by Mr. Kuul as shown in Table 5. He also summarized the key safety functions characteristic for the plants analyzed prior to the meeting as shown in Tables 6 and 7. Due to time limitations they could not be discussed, in particular to clarify certain statements that because of their brevity may be misunderstood such as in the case of the PIUS reactor. Mr. Ignatiev identified as positive trends in the development of advanced PWRs the increase of thermal margins and water inventories, long grace periods and the use of double containments. As for future work, the following topics for getting a better common understanding were suggested: use of passive and active safety systems; length of time safety systems (active or passive) are designed to work without operator intervention (e.g., grace periods for accident management); and the issue of severe accidents.

The beneficial safety features of the VPBER concept were emphasized by Mr. Dubrovin. They are based on the selection of an integral design which reduces the potential for a rapid loss of primary coolant on account of having no large-sized coolant lines

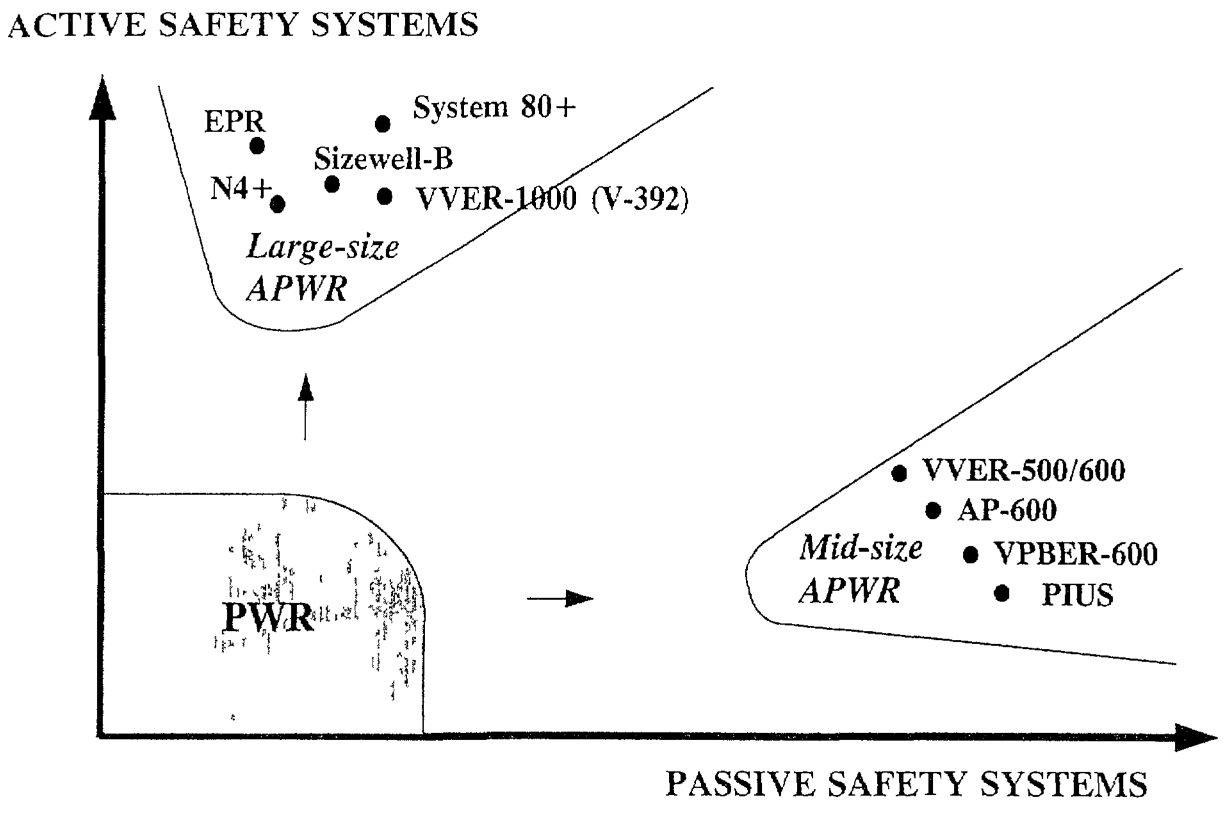


Fig. 1. Commonalities and dıfferences in design approaches

TABLE 5. COMMONALITIES AND DIFFERENCES IN DESIGN APPROACHES FOR ALWR

	COMMONALITIES	DIFFERENCES
LARGE ALWRs	● Coolant energy potential (temperature, pressure) ● Double containment ● Design pressure in containment	● Number of RCS loops ● Passive safety systems in V-392 ● Reduced core power density in APWR
MEDIUM ALWRs	● Coolant energy potential for evolutionary designs ● Reduced core power density ● Double protective barrier: double containment in many cases or guard vessel and containment	● Evolutionary and innovative designs (PIUS) ● Loop and integral layout of reactor (VPBER-600) ● Use of guard vessel and containment with reduced pressure in VPBER-600 ● Reduced RCS parameters in PIUS

connected to the primary system. In addition, the primary system is housed in a "guard vessel" which fits relatively tightly around the primary system, which in turn means that any small-sized primary coolant leaks that remain possible are terminated before the core becomes uncovered.

3.4. The difficulty of comparing "evolutionary" and "innovative" designs

This topic was addressed by Mr. Kramerov. He first stressed several important issues of a "philosophical" nature concerning new design approaches, and concluded with some practical design choices that.have to be made.

The observation was made that there is a need for discussing the evolutionary and innovative ("revolutionary") approaches, specifically to answer the question why one should change abruptly from existing reactor types to, e.g., new ones like PIUS. He pointed out that it would be very difficult, if not impossible, to make a meaningful comparison of evolutionary and innovative concepts. He also referred to the potential economic consequences that such an abrupt change may entail if it were to be made. In this context he also brought up the question of whether or not to reduce core power densitites, as already mentioned by Mr. Kukharkin. In addition, the usefulness of certain aspects of the severe

TABLE 6. SAFETY FUNCTIONS AND SYSTEMS OF ADVANCED LARGE POWER LIGHT WATER REACTORS

Safety function	**Emergency shutdown**	**Emergency core cooling (LOCA)**	**Emergency heat removal**	**Emergency containment cooling**
APWR	RCCA + active injection of absorber	4 accumulators + 4 trains of active ECCS	4 trains of active EFWS 4 trains of active RHR	4 trains of active ECCS
System 80+	RCCA + active injection of absorber	4 accumulators + 4 trains of active ECCS	4 trains of active EFWS 2 trains of active RHR + 2 backup pumps	2 trains of active ECCS + containment spray + 2 backup pumps
V - 392	RCCA + passive injection of absorber + active injection of absorber	4 accumulators + 4 tanks LP ECCS + 2 trains of active ECCS	4 trains of passive ERHRS to SG 4 trains of active EFWS	Active ECCS

Abbreviations: RCCA = rod cluster control assembly EFWS = emergency feed water supply GV = guard vessel
ERHRS = emergency residual heat removal system ECCS = emergency core cooling system RHR = residual heat removal

TABLE 7. SAFETY FUNCTIONS AND SYSTEMS OF ADVANCED MEDIUM POWER LIGHT WATER REACTORS

Safety function	Emergency shutdown	Emergency core cooling (LOCA)	Emergency heat removal	Emergency containment cooling
VPBER - 600	RCCA + passive injection of absorber + active injection of absorber	2 accumulators + GV + 4 trains of passive ERHRS	4 trains of passive ERHRS connected to reactor 2 trains of active RHR	---
MS - 600	RCCA + injection of liquid absorber	2 accumulators + 2 tanks LP ECCS + 2 trains of active LP ECCS	Active EFWS	---
PIUS	Passive injection of absorber from reactor pool	Feed of coolant from reactor pool	Passive bleed and feed of coolant 4 trains of passive ERHRS	---
AP - 600	RCCA + passive injection of absorber (LOCA)	2 HP tanks + 2 accumulators + 1 LP tank	Passive heat exchanger ERHR to reactor	Passive water-air cooling
V - 407	RCCA + passive injection of absorber	4 accumulators + 4 tanks LP ECCS	4 trains of passive ERHRS to SG 4 trains of active EFWS	2 trains of passive emergency containment cooling system
AC - 600	RCCA + passive injection of absorber + active injection of absorber	2 accumulators + 2 tanks HP ECCS + 4 trains of active LP ECCS	2 trains of passive ERHRS to SG	Passive water-air cooling

Abbreviations: RCCA = rod cluster control assembly EFWS = emergency feed water supply GV = guard vessel
ERHRS = emergency residual heat removal system ECCS = emergency core cooling system RHR = residual heat removal

accident discussion was questioned. In Mr. Kramerov's view, designs such as the AP600, or channel-type reactors such as the advanced Russian design, have sufficient safety features that core melt accidents need not be seriously considered. In other words, the emphasis is to be placed on (severe) accident prevention.

Concerning the practical choices that have to be made, he gave the following two examples: horizontal versus vertical steam generators, or pumps with or without flywheels (with shaft-seal or wet/canned motor). Or the question why Russian reactor vessels have coolant nozzles at two levels, whilst the western designs accommodate the necessary nozzles at a single level. He also pointed to the potential drawbacks of rapid depressurization systems, such as undesired actuation, either through erroneous operator action or through equipment malfunction.

As examples for currently still incomplete knowledge, needing appropriate development efforts, he mentioned the problem of injecting water into a "dry", overheated core, or the efforts needed to bring computer codes for analyzing very innovative concepts to a state that would be comparable to that achieved for those in use for current or near-term plants.

Regarding potential activities for the future, Mr. Kramerov suggested that attention should be given to advanced Russian channel type reactors and that they should be compared with other advanced channel type reactors such as the Canadian CANDU-3 or the Japanese ATR, and with vessel-type advanced PWRs. Such a comparison, drawing on the respective experiences, could be beneficial to all participating parties. He expressed the readiness to perform such work.

3.5. Accident prevention is an important subset of ALWR design approaches

The second part of the Workshop consisted in essence of responses to a number of observations and questions resulting from the previous session. The dominant themes were how to prevent by appropriate design features incidents from developing into accidents which could lead to fuel damage. Should this occur nevertheless, the issue is how the consequences of such fuel damage can best be mitigated. Even so, it was strongly stressed by several speakers that the designs of advanced plants have many other important objectives. In summary these concern ease of operation and maintenance, flexibility of operation, and competitiveness with other means of large-scale electricity generation.

The general discussion was opened by Mr. Lang. He addressed two different topics. The first one concerned the suitability of INSAG-3 principles as a basis for the review of the adequacy of the safety provisions in the design of advanced reactor plants. Whilst he concurred that the structure chosen in this document for addressing the 15 key design areas selected is useful for reviewing future plants, he strongly questioned the usefulness of the 50 specific principles for countries with a comprehensive and well established programme of safety regulation. The essential reasons are given in Table 8. In essence, the principles are too general to be used as yardsticks for advanced plants, since they were written for earlier, operating plants and had to accommodate all the designs in operation when the document was published in 1988.

In response to some observations made during the TCM, he pointed out that filtered venting of the containment was a backfitting measure taken in some countries to meet severe

TABLE 8. COMMENTS ON INSAG-3 AND INSAG-5

INSAG-3 - 1988

- Contains "the basic safety principles for existing and future reactor types" and was prepared "to formulate, where possible, commonly shared safety concepts."
- Contains objectives (3) and principles (12 fundamental, 50 specific).
- "These principles do not constitute a set of regulatory requirements." They "are stated on the assumption that practices are in current use."
- Are generalizations of NRC and other nationally observed principles.
- Consequently, any design that conforms to NRC (or other national) principles must also conform to the INSAG-3 principles.

INSAG-5 - 1992

- Contains chapters on "Features Desired in Future Plants" and "Continued Improvement of Nuclear Power Plant Safety."
- States that the principles of INSAG-3 should become mandatory.
- Discusses pros and cons of future design trends, without taking positions on the more controversial issues.
- Consequently, does not effectively expand on the principles of INSAG-3.

Conclusion

Neither document provides meaningful guidance to designers of advanced plants in countries already subject to detailed, comprehensive nuclear safety regulation.

accident concerns of operating plants that arose after the TMI accident. He stressed that in the USA severe accidents are being considered at the design stage of advanced plants and that the containments are designed for the resulting challenges without filtered vents. Since filtered venting involves more or less controlled release, it is basically less desirable than complete containment without any release.

With regard to the question of evolutionary vs. innovative designs, he indicated that because U.S. utilities are subject to strict economic regulation they are extremely risk-averse, and consequently strongly prefer evolutionary designs, for which the risks are considered much smaller than for innovative concepts (e.g., PIUS). For this purpose, both the so-called Evolutionary and Passive designs in the United States fall into the "evolutionary" category.

With respect to the long-term durability of large thermal design margins (a question that had already been raised by Mr. Kramerov), Mr. Lang stated his personal view, not universally shared by others in the U.S., that such margins represented a valuable asset that can be used for a number of desirable purposes in an operating plant. Hence, it is questionable whether the margins now being provided in the advanced designs will actually be retained throughout the life of the corresponding plants.

As to the question of active versus passive design features, he observed that either can in principle be used to achieve any target reliability. The choice should be made on the basis of which solution provides that reliability at lowest cost for any specific application.

Furthermore, the impetus for passive features in the U.S. originated from the desire of many utilities for smaller units. It was thought that passive systems, which in many applications have inherent size limitations, would allow sufficient simplification in the mid-size plants so as to counteract the economies of scale in comparison to the large plants. The apparent association of passive with mid-size and active with large-size is therefore perhaps more a result of the history of the designs than of any inherent technical reasons.

Mr. Ritterbusch supported the previous speaker in many points and added others of his own. He stressed the necessity of establishing a proper balance between accident prevention and accident mitigation in any design approach. As to the ultimate safety objective he said that as a designer he would ideally like to show that his plant is so safe that no off-site emergency measures would be needed. Realistically, however, he expects simplification of emergency plans, but does not expect regulators to permit complete omission of emergency plans, regardless of such showing.

Designing against the consequences of severe accidents has its special problems as the knowledge of the physical phenomena involved is not very good. This means that the specific design approaches involve a judicious combination of conservative assumptions, hand calculations, engineering judgement and providing a robust design.

As to the role of the operator in the case of severe accidents, Mr. Ritterbusch pointed out that both the Evolutionary and the Passive plants are designed in a way that such accidents can be mitigated without early intervention of the operator. The operator should have the possibility of taking actions if desired. For this, however, the operator would need proper information which requires that adequate instrumentation and information processing is provided in the design. Regarding instrumentation and control in general, there is a strong trend towards full digitization and information processing to assist the operator in making decisions in an optimal way during normal operation and in case of abnormal occurrences.

To illustrate how much margin advanced plants have built-in, the results of best-estimate analyses for System 80+ show that, even though the design basis is 0.3 g, seismic events can be withstood up to 0.7 g without significant likelihood of reactor core damage. This particular example was quoted since earthquakes are viewed as the most important of the external events.

Several other speakers from Western countries largely concurred with the statements made before even though there were differences in emphasis and certain positions. For example in regard to what freedom should be given the operator for dealing with accidents, Mr. Czech referred to research results showing that operators often think that their assessment of a situation is correct whilst in reality it is not. It is a human attitude to defend the first decision taken although additional information obtained afterwards requires a new assessment of the situation. As a consequence, Mr. Czech pleaded for a very high degree of automation in accident prevention and mitigation. Another area of difference in positions concerns the question of whether or not the option of filtered containment venting should be kept open as an ultimate mitigation measure for advanced plants.

As much emphasis was placed during the discussion on severe accidents, both with regard to prevention and mitigation, Mr. Yvon reminded the audience that this is only one aspect of the topic of design approaches for advanced light water reactors. Design for good constructability, ease and flexibility of operation and maintenance, and for competitively low cost are equally important considerations. As to "passivity", he pointed out that this cannot be an objective in itself but only a means for accomplishing a desired function, and a selection has to be made by evaluating the respective merits case by case.

Responding to the main theme of the discussion, Mr. Yvon observed that prevention, meaning in essence design for low core damage frequencies, entails the proper consideration of important points such as:

- low contribution of external hazards such as earthquakes;
- reduction of common mode failures through appropriate layout and system configuration, including support systems;
- incorporating inspection and maintenance constraints and, in addition;
- considering all reactor states, including shutdown;
- covering sequences of low probability (multiple failures).

Regarding severe accident mitigation the key question is how much should be done. The Franco-German position was introduced in the EPR presentation as a specific example.

3.6. Common position on accident mitigation

In response to a Russian question it was stated that in all Western countries severe accidents have to be considered for future plants. As to severe accident mitigation, Mr. Berger summarized a commonly shared understanding as follows:

- In many countries the mitigation of core melting will be required by regulators whatever the quality and extent of the prevention is.
- Experimental and analytical research and development, which has been performed in the past mainly to support current plants, will allow a better understanding of the physical phenomena and appropriate countermeasures in future plants.
- In this context it is important to identify the phenomena that must be dealt with and also the bounds of assumptions. For these, a limit has to be found, that is, the "what if game" must be kept within reasonable bounds.
- For practical application, realistic analyses have to be performed and engineering judgement has to be used. Analytical tools (such as PSAs) have to be improved in order to be able to design severe accident mitigation features.
- Information (as reliable as possible) has to be provided to the operators and the emergency response teams.
- The plants are to be designed with a grace period that provides ample time for mitigative actions before a potentially large release might occur.
- Everything has to be done technically to reduce (minimize) the emergency plans but their implementation in the different countries is often a political problem.

4. CONCLUSIONS

Although many differences in design approaches were in evidence throughout the TCM, a number of common themes could be identified among many of the design approaches presented. These included further improvements with regard to safety, design simplification, reduction in cost, incorporation of feedback from operating experience, and control room improvements with respect to human factors and digitization. Safety improvements included the consideration of severe accidents from the beginning of the design process, increased thermal margins and water inventories, longer grace periods, and double containments, all of which serve to enhance safety in probabilistic terms by more than one order of magnitude, in comparison to operating plants.

The latest Status Report (TECDOC 479) on different advanced light water reactor designs was published in 1988, the same year that INSAG-3 appeared. It is evident from the material presented at this TCM that much progress has been made for a number of plant designs. They are all in conformance with the basic principles of INSAG-3 for design aspects. But for the other points of INSAG-3, such as quality of construction, in-service inspection and maintenance, they cannot effectively be reviewed at this stage.

Improving the management of severe accidents, a characteristic trend in the development of future reactors, is being given much emphasis, but similar emphasis needs to be placed on the effect of such improvements on capital cost. Whilst improvements concerning prevention are certain and predictable, the mitigation of severe accidents is relatively more uncertain. For this reason it seems necessary to evaluate more carefully the inputs of R&D laboratories to the design, as their interests are different from those of the nuclear industry, utilities included.

The second important point concerns the utilization of margins. There is a need to find a balance between large margins and cost. What margins have to be established is a problem between regulators, designers, and utilities. For the latter the margin requirements are dictated particularly by the grid conditions and by operational aspects as well as by safety considerations.

The third point concerns instrumentation and control, and the computerization of the control room. For example, a very large effort has been made in France. But repercussions were found with regard to cost. Large difficulties were experienced regarding qualification with the consequence that an "old system" had to be added as a backup to the new system. Again, there is a need to moderate such type of "evolution".

The final point concerned the PSA-approach. Whilst the INSAG-recommendations regarding target values for core damage frequencies and for the probability of a large release appear to be reasonable, it is difficult to attain them in practice. It is important to also put a limit to these objectives and to the corresponding target values. The effects of common mode failures and of human errors seem to set the related limits. It is important to find a consensus, particularly as far as PSA-levels 2 and 3 are concerned, because the results depend to a large degree on the methodologies used and the hypotheses postulated.

At the end of the TCM and the Workshop Mr. Ponomarev-Stepnoi, the General Chairman of both meetings, summarized the presentations and discussions by noting that the design of advanced nuclear power plants is quite obviously progressing, and that the information exchange at the TCM was very useful for improved understanding of different design approaches. He recommended this kind of discussion and information exchange to be continued, with inclusion of possible new designs. Furthermore, he suggested a closer cooperation between designers and regulators be established, through the organization of meetings between regulators from different countries, possibly also with participation of designers, to attain a mutual understanding of different approaches and requirements.

Several suggestions for further activities were made during the Workshop. Primarily they concern cross-cutting studies that go into greater detail as to how the various designs or design concepts differ in the 15 key design areas addressed in the papers.

Part II
CORRESPONDENCE BETWEEN INSAG-3 AND US-NRC REGULATORY GUIDE 1.70

The design descriptions for the various ALWR presented in part III of this report generally follow the structure that the International Nuclear Safety Advisory Group (INSAG) to the Director General of the IAEA has selected in their document "Basic Safety Principles for Nuclear Power Plants, INSAG-3" for addressing the key areas of plant design. As the design and licensing practice in many countries follows the approach taken in the USA it was considered very helpful for the reader of this TECDOC to have a cross-reference between the criteria of the Regulatory Guide 1.70 of the US-NRC and the corresponding INSAG-3 design principles. This cross reference was prepared by B.A. Mclntyre of Westinghouse Electric Corporation as part of the description of AP-600. The sequence selected is identical to the sub-headings of section 2 of each individual plant description presented in part III of this TECDOC.

In the subsequent discussion only the related INSAG-3 Principle is stated in italics even though the accompanying explanations given in the INSAG document are also needed for a thorough understanding. As it can be assumed that most readers of this TECDOC have the INSAG document available, these extensive explanations are not repeated in the current TECDOC.

US-NRC Requirements related to INSAG-3 principles

INSAG-3 Principle: 4.2.2.1. Plant process control systems

> *Normal operation and anticipated operational occurences are controlled so that plant and system variables remain within these operating ranges. This reduces the frequency of demands on the safety systems.*

The U.S. NRC requirements that are relevant to this principle include the following General Design Criteria:

General Design Criterion 10 - Reactor Design

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

General Design Criterion 12 - Suppression of Reactor Power Oscillations

The reactor core and associated coolant, control, and protection systems shall be designed to assure that power oscillations which can result in conditions exceeding specified acceptable fuel design limits are not possible or can be reliably and readily detected and suppressed.

General Design Criterion 13 - Instrumentation and Control

Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

General Design Criterion 15 - Reactor Coolant System Design

The reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during normal operation, including anticipated operational occurrences.

General Design Criterion 19 - Control Room

A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss of coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent, to any part of the body, for the duration of the accident.

Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

General Design Criterion 24 - Separation of Protection and Control Systems

The protection system shall be separated from the control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

General Design Criterion 26 - Reactivity Control System Redundancy and Capability

Two independent reactivity control systems of different design principles shall be provided. One of the systems shall use control rods, preferably including a positive means for inserting the rods, and shall be capable of reliably controlling reactivity changes to assure that under conditions of normal operation, including anticipated operational occurrences, and with appropriate margin for malfunctions such as stuck rods, specified acceptable fuel design limits are not exceeded. The second reactivity control system shall be capable of reliably controlling the rate of reactivity changes resulting from planned, normal power changes (including xenon burnout) to assure that the acceptable fuel design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions.

General Design Criterion 27 - Combined Reactivity Control Systems Capability

The reactivity control systems shall be designed to have a combined capability, in conjunction with poison addition by the emergency core cooling system, of reliably controlling reactivity changes to assure that under postulated accident conditions and with appropriate margin for stuck rods the capability to cool the core is maintained.

General Design Criterion 28 - Reactivity Limits

The reactivity control systems shall be designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor coolant pressure boundary greater than limited local yielding nor (2) sufficiently disturb the core, its support structures, or other reactor pressure vessel internals to impair significantly the capability to cool the core. These postulated reactivity accidents shall include consideration of rod ejection (unless prevented by positive means), rod dropout, steam line rupture, changes in reactor coolant temperature and pressure, and cold water addition.

General Design Criterion 29 - Protection Against Anticipated Operational Occurrences

The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.

INSAG-3 Principle: 4.2.2.2 Automatic safety systems

> *Automatic systems are provided that would safely shut down the reactor, maintain it in a cooled state, and limit any release of fission products that might possibly ensure, if operating conditions were to exceed predetermined setpoints.*

Relevant US NRC Requirements:

The U.S. NRC requirements that are relevant to this principle include the following General Design Criteria:

General Design Criterion 13 - Instrumentation and Control

Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

General Design Criterion 17 - Electrical Power Systems

An on-site electric power system and an off-site electric power system shall be provided to permit functioning of structures, systems, and components important to safety. The safety function for each system (assuming that the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents.

The onsite electric power supplies, including the batteries, and the onsite electric distribution system shall have sufficient independence, redundancy, and testability to perform their safety functions, assuming a single failure.

Electric power from the transmission network to the onsite electric distribution system shall be supplied by two physically independent circuits (not necessarily on separate rights of way) designed and located so as to minimize, to the extent practical, the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions. A switchyard common to both circuits is acceptable. Each of these circuits shall be designed to be available in sufficient time, following a loss of all onsite alternating current power supplies and other offsite electric power circuit, to assure that specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded. One of these circuits shall be designed to be available within a few seconds following a loss of coolant accident to assure that core cooling, containment integrity, and other vital safety functions are maintained.

Provisions shall be included to minimize the probability of losing electric power from any of the remaining supplies as a result of, or coincident with, the loss of power generated by the nuclear power unit, the loss of power from the transmission network, or the loss of power from the onsite electric power supplies.

General Design Criterion 22 - Protection System Independence

The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in the loss of the protection function or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

General Design Criterion 23 - Protection System Failure Modes

The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air) or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.

General Design Criterion 24 - Separation of Protection and Control Systems

The protection system shall be separated from the control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

General Design Criterion 35 - Emergency Core Cooling

A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (l) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts.

Suitable redundancy in components and features and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

General Design Criterion 37 - Testing of Emergency Core Cooling System

The emergency core cooling system shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leak-tight integrity of its components, (2) the operability and performance of the active components of the system, and (3) the operability of the system as a whole and under conditions as close to design as practical, the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.

INSAG-3 Principle: 4.2.3.1 Protection against power transient accidents

> *The reactor is designed so that reactivity induced accidents are protected against, with a conservative margin of safety*

Relevant US NRC Requirements:

The following US NRC requirements that are relevant to this principle include the following General Design Criteria:

Criterion 10 - Reactor Design

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

Criterion 11 - Reactor Inherent Protection

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

Criterion 12 - Suppression of Reactor Power Oscillations

The reactor core and associated coolant, control, and protection systems shall be designed to assure that power oscillations which can result in conditions exceeding specified acceptable fuel design limits are not possible or can be reliably and readily detected and suppressed.

Criterion 13 - Instrumentation and Control

Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall provided to maintain these variables and systems within prescribed operating ranges.

Criterion 20 - Protection System Functions

The protection system shall be designed (1) to Initiate automatically the operation of appropriate systems, including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

Criterion 21 - Protection System Reliability and Testability

The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in the loss of the protection function and (2) removal from service of any component or channel does not result in the loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

Criterion 22 - Protection System Independence

The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in the loss of the protection function or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

Criterion 23 - Protection System Failure Modes

The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air) or postulated adverse environments (e.g.. extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.

Criterion 24 - Separation of Protection and Control Systems

The protection system shall be separated from the control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

Criterion 25 - Protection System Requirements for Reactivity Control Malfunctions

The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of the control rods.

Criterion 26 - Reactivity Control System Redundancy and Capability

Two independent reactivity control systems of different design principles shall be provided. One of the systems shall use control rods, preferably including a positive means for inserting the rods, and shall be capable of reliably controlling reactivity changes to assure that under conditions of normal operation, including anticipated operational occurrences, and with appropriate margin for malfunctions such as stuck rods, specified acceptable fuel design limits are not exceeded. The second reactivity control system shall be capable of reliably controlling the rate of reactivity changes resulting from planned, normal power changes (including xenon burnout) to assure that the acceptable fuel design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions.

Criterion 27 - Combined Reactivity Control Systems Capability

The reactivity control systems shall be designed to have a combined capability, in conjunction with poison addition by the emergency core cooling system, of reliably controlling reactivity changes to assure that under postulated accident conditions and with appropriate margin for stuck rods the capability to cool the core is maintained.

Criterion 28 - Reactivity Limits

The reactivity control systems shall be designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor coolant pressure boundary greater than limited local yielding nor (2) sufficiently disturb the core, its support structures, or other reactor pressure vessel internals to impair significantly the capability to cool the core. These postulated reactivity accidents shall include consideration of rod ejection (unless prevented by positive means), rod dropout, steam line rupture, changes in reactor coolant temperature and pressure, and cold water addition.

Criterion 29 - Protection Against Anticipated Operational Occurrences

The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.

INSAG-3 Principle: 4.2.3.2 Reactor core integrity

> *The core is designed to have mechanical stability. It is designed to tolerate an appropriate range of anticipated variations in operational parameters. The core design is such that the expected core distortion or movement during an accident within the design basis would not impair the effectivenss of the reactivity control or the safety shutdown systems or prevent cooling of the fuel.*

Relevant US NRC Requirements:

The U.S. NRC requirements that are relevant to this principle include the following General Design Criteria:

Criterion 1 - Quality Standards and Records

Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety function to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified, as necessary, to assure a quality product, in keeping with the required safety function. A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

Criterion 2 - Design Bases for Protection Against Natural Phenomena

Structures, systems; and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without the loss of the capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena, and (3) the importance of the safety functions to be performed.

Criterion 4 - Environmental and Missile Design

Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit.

Criterion 10 - Reactor Design

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

10CFR50.46

The acceptance criteria for loss of Coolant Accidents are defined in 10CFR50.46 as follows:

- The calculated maximum fuel element cladding temperature shall not exceed 2200°F.
- Localized cladding oxidation shall not exceed 17 percent of the total cladding thickness before oxidation.
- The amount of hydrogen generated from fuel element cladding reacting chemically with water or steam shall not exceed one percent of the total amount if all metal cladding were to react.
- The core remains amenable to cooling for any calculated change in core geometry.
- The core temperature is maintained at a low value and decay heat is removed for the extended period of time required by the long-lived radioactivity remaining in the core.

INSAG-3 Principle: 4.2.3.3 Automatic shutdown systems

> *Rapidly responding and highly reliable reactivity reduction for safety purposes is designed to be independent of the equipment and processes used to control the reactor power. Safety shutdown action is available at all times when steps to achieve a self-sustaining chain reaction are being intentionally taken or whenever a chain reaction might be initiated accidentally.*

Relevant US NRC Requirements:

Criterion 24 - Separation of Protection and Control Systems

The protection system shall be separated from the control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

Criterion 27 - Combined Reactivity Control Systems Capability

The reactivity control systems shall be designed to have a combined capability, in conjunction with poison addition by the emergency core cooling system, of reliably controlling reactivity changes to assure that under postulated accident conditions and with appropriate margin for stuck rods the capability to cool the core is maintained.

INSAG-3 Principle: 4.2.3.4 Normal heat removal

> *Heat transport systems are designed for highly reliable heat removal in normal operation. They would also provide means for the removal of heat from the reactor core during anticipated operational occurrences and during most types of accidents that might occur.*

Relevant US NRC Requirements:

The US NRC requirements that are relevant to this principle include the following General Design Criteria:

General Design Criterion 1 - Quality Standards and Records

Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety function to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified, as necessary, to assure a quality product, in keeping with the required safety function. A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

General Design Criterion 2 - Design Bases for Protection Against Natural Phenomena

Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without the loss of the capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena, and (3) the importance of the safety functions to be performed.

General Design Criterion 4 - Environmental and Missile Design Bases

Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit.

General Design Criterion 5 - Sharing of Structures, Systems, and Components

Structures, systems, and components important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, 11 in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining unit.

General Design Criterion 10 - Reactor Design

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

General Design Criterion 11 - Reactor Inherent Protection

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

General Design Criterion 14 - Reactor Coolant Pressure Boundary

The reactor coolant pressure boundary shall be designed, fabricated, erected, and tested so as to have an extremely low probability of abnormal leakage, of rapidly propagating failure, and of gross rupture.

General Design Criterion 15 - Reactor Coolant System Design

The reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during normal operation, including anticipated operational occurrences.

General Design Criterion 30 - Quality of Reactor Coolant Pressure Boundary

Components which are part of the reactor coolant pressure boundary shall be designed, fabricated, erected, and tested to the highest quality standards practical. Means shall be provided for detecting and, to the extent practical, identifying the location of the source of reactor coolant leakage.

General Design Criterion 31 - Fracture Prevention of Reactor Coolant Pressure Boundary

The reactor coolant pressure boundary shall be designed with sufficient margin to assure that when stressed under operating, maintenance, testing, and postulated accident conditions (1) the boundary behaves in a nonbrittle manner and (2) the probability of rapidly propagating fracture is minimized. The design shall reflect consideration of service temperatures and other conditions of the boundary material under operating, maintenance, testing, and postulated accident conditions and the uncertainties in deterring (1) material properties, (2) the effects of irradiation on material properties, (3) residual, steady state, and transient stresses, and (4) size of flaws.

General Design Criterion 32 - Inspection of Reactor Coolant Pressure Boundary

Components which are part of the reactor coolant pressure boundary shall be designed to permit (1) periodic inspection and testing of important areas and features to asks their structural and leak-tight integrity and (2) an appropriate material surveillance program for the reactor pressure vessel.

General Design Criterion 33 - Reactor Coolant Makeup

A system to supply reactor coolant makeup for protection against small breaks in the reactor coolant pressure boundary shall be provided. The system safety function shall be to assure that specified acceptable fuel design limits are not exceeded as a result of reactor coolant loss due to leakage from the reactor coolant pressure boundary and rupture of small piping or other small components which are part of the boundary. The system shall be designed to assure that for on-site electric power system operation (assuming off-site power is not available) and for off-site electric power system operation (assuming on-site power is not available) the system safety function can be accomplished using the piping, pumps, and valves used to maintain coolant inventory during normal reactor operation.

General Design Criterion 34 - Residual Heat Removal

A system to remove residual heat shall be provided. The system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified acceptable fuel design limits and the design conditions of the reactor coolant pressure boundary are not exceeded.

Suitable redundancy in components and features and suitable interconnections, leak detection, and isolation capabilities shall he provided to assure that for on-site electric power system operation (assuming off-site power is not available) and for off-site electric power system operation (assuming on-site power is not available) the system safety function can be accomplished, assuming a single failure.

INSAG-3 Principle: 4.2.3.5 Emergency heat removal

> *Provision is made for alternative means to restore and maintain fuel cooling under accident conditions, even if normal heat removal fails or the integrity of the primary cooling system boundary is lost.*

Relevant - US NRC Requirements:

The U.S. NRC requirements that are relevant to this principle include the following General Design Criteria:

General Design Criterion 35 - Emergency Core Cooling

A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts.

Suitable redundancy in components and features and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

General Design Criterion 38 - Containment Heat Removal System

A system to remove heat from the reactor containment shall be provided. The system safety function shall be to reduce rapidly, consistent with the functioning of other associated system, the containment pressure and temperatures, following any loss of coolant accident and maintain them at acceptably low levels.

Suitable redundancy in components and features and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that for on-site electrical power system operation (assuming off-site power is not available) and for off-site electrical power system operation (assuming on-site power is not available) the system safety function can be accomplished, assuming a single failure.

INSAG-3 Principle: 4.2.3.6 Reactor coolant system integrity

> *Codes and standards for nuclear vessels and piping are supplemented by additional measures to prevent conditions arising that could lead to a rupture of the primary coolant system boundary at any time during the operational life of the plant.*

Relevant US NRC Requirements:

The US NRC requirements that are relevant to this principle include the following General Design Criteria:

General Design Criterion 1 - Quality standards and records

Structures, systems, and components important to safety shall he designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety function to he performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified, as necessary, to assure a quality product, in keeping with the required safety function. A quality assurance program shall he established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall he maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

General Design Criterion 14 - Reactor Coolant Pressure Boundary

The reactor coolant pressure boundary shall be designed, fabricated, erected, and tested so as to have an extremely low probability of abnormal leakage, of rapidly propagating failure, and of gross rupture.

General Design Criterion 15 - Reactor coolant system design

The reactor coolant system and associated auxiliary, control, and protection systems shall he designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during normal operation, including anticipated operational occurrences.

General Design Criterion 30 - Quality of reactor coolant pressure boundary

Components which are part of the reactor coolant pressure boundary shall he designed, fabricated, erected, and tested to the highest quality standards practical. Means shall he provided for detecting id, to the extent practical, identifying the location of the source of reactor coolant leakage.

General Design Criterion 31 - Fracture prevention of reactor coolant pressure boundary

The reactor coolant pressure boundary shall be designed with sufficient margin to assure that when stressed under operating, maintenance, testing, and postulated accident conditions (l) the boundary behaves in a nonbrittle manner and (2) the probability of rapidly propagating fracture is minimized. The design shall reflect consideration of service temperatures and other conditions of the boundary material under operating, maintenance, testing, and postulated accident conditions and the uncertainties in determining (l) material properties, (2) the effects of irradiation on material properties, (3) residual, steady state, and transient stresses, and (4) size of flaws.

General Design Criterion 32 - Inspection of reactor coolant pressure boundary

Components which are part of the reactor coolant pressure boundary shall be designed to permit (l) periodic inspection and testing of important areas and features to assess their structural and leak-tight integrity and (2) an appropriate material surveillance program for the reactor pressure vessel.

Title 10 of the Code of Federal Regulations Section 50.55a (10 CFR 50.55a) - Codes and standards includes the requirement that the pressure boundary be designed and constructed in accordance with the requirements of the ASME Boiler and Pressure Vessel Code, Section III.

INSAG-3 Principle: 4.2.3.7 Confinement of radioactive material

> *The plant is designed to be capable of retaining the bulk of the readioactive material that might be released from fuel, for the entire range of accidents considered in the design.*

Relevant US NRC Requirements:

Criterion 1 - Quality Standards and Records

Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety function to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified, as necessary, to assure a quality product, in keeping with the required safety function.

A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

Criterion 16 - Containment Design

The reactor containment and associated systems shall be provided to establish an essentially leak-tight barrier against the uncontrolled release of radioactivity to the environment and to assure that the containment design conditions Important to safety are not exceeded for as long as postulated accident conditions require.

Criterion 38 - Containment Heat Removal System

A system to remove heat from the reactor containment shall be provided. The system safety function shall be to reduce rapidly, consistent with the functioning of other associated systems, the containment pressure and temperature following any loss of coolant accident and maintain them at acceptably low levels.

Suitable redundancy in components and features and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that for on-site electrical power system operation (assuming off-site power is not available) and for off-site electrical power system operation (assuming on-site power is not available) the system safety function can be accomplished, assuming a single failure.

Criterion 39 - Inspection of Containment Heat Removal System

The containment heat removal system shall be designed to permit appropriate periodic inspection of important components, such as the tons, sumps, spray nozzles and piping to assure the integrity and capability of the system.

Criterion 40 - Testing of Containment Heat Removal System

The containment heat removal system shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leaktight integrity of its components, (2) the operability and performance of the active components of the system, and (3) the operability of the system as a whole, and, under conditions as close to the design as practical the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.

Criterion 41 - Containment Atmosphere Cleanup

Systems to control fission products, hydrogen, oxygen, and other substances which may be released into the reactor containment shall be provided, as necessary, to reduce, consistent with the functioning of other associated systems, the concentration and quantity of fission products released to the environment following postulated accidents and to control the concentration of hydrogen or oxygen and other substances in the containment atmosphere following postulated accidents to assure that containment integrity is maintained.

Each system shall have suitable redundancy in components and features and suitable interconnections, leak detection, isolation, and containment capabilities to assure that for on-site electric power system operation (assuming off-site power is not available) and for off-site electric power system operation (assuming on-site power is not available) its safety function can be accomplished, assuming a single failure.

Criterion 42 - Inspection of Containment Atmosphere Cleanup System

The containment atmosphere cleanup systems shall be designed to permit appropriate periodic inspection of important components such as filter frames, ducts, and piping, to assure the integrity and capability of the systems.

Criterion 43 - Testing of Containment Atmosphere Cleanup Systems

The containment atmosphere cleanup systems shall be designed to permit appropriate periodic pressure and functional testing to assure (l) the structural and leak-tight integrity of its components, (2) the operability and performance of the active components of the systems such as fans, filters, dampers, pumps, and valves, and (3) the operability of the systems as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the systems into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of associated systems.

Criterion 50 - Containment Design Basis

The reactor containment structure, including access opening, penetrations, and the containment heat removal system, shall be designed so that the containment structure and its internal compartments can accommodate, without exceeding the design leakage rate and with sufficient margin, the calculated pressure and temperature conditions resulting from any loss of coolant accident. This margin shall reflect consideration of (l) the effects of potential energy sources which have not been included in the determination of the peak conditions, such as energy in steam generators and energy from metal-water and other chemical reactions that may result from degraded emergency core cooling functioning. (2) the limited experience and experimental data available for defining accident phenomena and containment responses, and (3) the conservatism of the calculational model and input parameters.

Criterion 51 - Fracture Prevention of Containment Pressure Boundary

The reactor containment boundary shall be designed with sufficient margin to assure that under operating. Maintenance, testing, and postulated accident conditions (1) its ferritic materials behave in a nonbrittle manner and (2) the probability of rapidly propagating fracture is minimized. The design shall reflect consideration of service temperatures and other conditions of the containment boundary material during operation, maintenance, testing, and Postulated accident conditions, and the uncertainties in determining (1) material properties, (2) residual, steady-state, and transient stresses, and (3) size of flaws.

Criterion 52 - Capability for Containment Leakage Rate Testing

The reactor containment and other equipment which may he subjected to containment test conditions shall be designed so that periodic integrated leakage rate testing can be conducted at containment design pressure.

Criterion 53 - Provisions for Containment Testing and Inspection

The reactor containment shall be designed to permit (1) appropriate periodic inspection of all important areas, such as penetrations, (2) an appropriate surveillance program, and (3) periodic testing at containment design pressure of the leak-tightness of penetrations which have resilient seals and expansion bellows.

Criterion 54 - Piping Systems Penetrating Containment

Piping systems penetrating the primary reactor containment shall be provided with leak detection, isolation and containment capabilities having redundancy, reliability, and performance capabilities which reflect the importance to safety of isolating these piping systems. Such piping systems shall be designed with a capability to test periodically the operability of the isolation valves and associated apparatus and to determine if valve leakage is within acceptable limits.

Criterion 55 - Reactor Coolant Pressure Boundary Penetrating Containment

Each line that is part of the reactor coolant pressure boundary and that penetrates primary reactor containment shall be provided with containment isolation valves as follows, unless it can be demonstrated that the containment isolation provisions for a specific class of lines, such as instrument lines, are acceptable on some other defined basis:

1. One locked closed isolation valve inside and one locked closed isolation valve outside containment; or
2. One automatic isolation valve inside and one locked closed isolation valve outside containment; or
3. One locked closed isolation valve inside and one automatic isolation valve outside the containment. A simple check valve may not be used as the automatic isolation valve outside containment; or
4. One automatic isolation valve inside and one automatic isolation valve outside containment. A simple check valve may not be used as the automatic isolation valve outside containment.

Isolation valves outside containment shall be located as close to containment as practical and, upon loss of actuating power, automatic isolation valves shall be designed to take the position that provides greater safety.

Other appropriate requirements to minimize the probability or consequences of an accidental rupture of these lines or of lines connected to them shall be provided, as necessary, to assure adequate safety. Determination of the appropriateness of these requirements, such as higher quality in design, fabrication, and testing, additional provisions for in-service inspection, protection against more severe natural phenomena, and additional isolation valves and containment, shall include consideration of the population density, and use characteristics, and physical characteristics of the site environs.

Criterion 56 - Primary Containment Isolation

Each line that connects directly to the containment atmosphere and penetrates the primary reactor containment shall be provided with containment isolation valves as follows, unless it can be demonstrated that the containment isolation provisions for a specific class of lines, such as instrument lines, are acceptable on some other defined basis:

1. One locked closed isolation valve inside and one locked closed isolation valve outside the containment; or
2. One automatic isolation valve inside and one locked closed isolation valve outside the containment; or
3. One locked closed isolation valve inside and one automatic isolation valve outside the containment. A simple check valve may not be used as the automatic isolation valve outside containment; or
4. One automatic isolation valve inside and one automatic isolation valve outside the containment. A simple check valve may not be used as the automatic isolation valve outside the containment.

Isolation valves outside the containment shall be located as close to the containment as practical id, upon loss of actuating power, automatic isolation valves shall be designed to take the position that provides greater safety.

Criterion 57 - Closed System Isolation Valves

Each line that penetrates the primary reactor containment and is neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere shall have at least one containment isolation valve which shall be either automatic, locked closed, or capable of remote manual operation. This valve shall be outside the containment and located as close to the containment as practical. A simple check valve may not be used as the automatic Isolation valve.

INSAG-3 Principle: 4.2.3.8 Protection of confinement structure

> *If specific and inherent features of a nuclear power plant would not prevent detrimental effects on the confinement structure in a severe accident, special protection against the effects of such accidents is provided, to the extent needed to meet the general safety objective.*

Relevant US NRC Requirements:

NRC Policy Issue SECY-93-087 "Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs" specifies:

As discussed in SECY-90-016, the staff recommended that the Commission approve the position to evaluate evolutionary ALWR's using a conditional containment failure probability (CCFP) of 0.1, or a deterministic containment performance goal that offers comparable protection. The NRC safety goal for core melt frequency is $1x10^{-4}$ per reactor year]. The Staff concluded that the general criterion would be an appropriate substitute for a CCFP in evaluating evolutionary ALWR containment performance during a severe-accident challenge:

The containment should maintain its role as a reliable, leak-tight barrier by ensuring that the containment stresses do not exceed ASME service level C limits for a minimum period of 24 hours following the onset of core damage, and that following this 24 hour period the containment should continue to provide a barrier against the uncontrolled release of fission products.

The staff proposed this containment performance goal to ensure that the containment will perform its function in the face of most credible severe accident challenges.

INSAG-3 Principle: 4.2.3.9 Monitoring of plant safety status

> *Parameters to be monitored in the control room are selected, and their displays are arranged, to ensure that operators have clear and unambiguous indications of the status of plant conditions important for safety, especially for the purpose of identifying and diagnosing the automatic actuation and operation of a safety system or the degradation of defense in depth.*

Relevant US NRC Requirements:

Criterion 13 - Instrumentation and Control

Instrumentation shall be provided to monitor variables and system over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and system that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment id its associated system. Appropriate controls shall be provided to maintain these variables and system within prescribed operating ranges.

INSAG-3 Principle: 4.2.3.10 Preservation of control capability

> *The main control room is designed to remain habitable under normal operating conditions anticipated abnormal occurrences and accidents considered in the design. Independent monitoring and the essential capability for control needed to maintain ultimate cooling, shutdown and confinement are provided remote from the main control room for circumstances in which the main control room may be uninhabitable or damaged.*

Relevant US NRC Requirements:

Criterion 1 - Quality Standards and Records

Structures, system, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety function to be performed. Where generally recognized codes and standards - used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified, as necessary, to assure a quality product, in keeping with the required safety function.

A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, system, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, system, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

Criterion 19 - Control Room

A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss of coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent, to any part of the body, for the duration of the accident.

Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown and

(2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

INSAG-3 Principle: 4.2.3.11 Station Blackout

> *Nuclear plants are so designed that the simultaneous loss of normal on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage.*

Relevant US NRC Requirements:

General Design Criterion 17 - Electrical Power Systems

An on-site electric power system and a off-site electric power system shall be provided to permit functioning of structures, system, and components important to safety. The safety function for each system (assuming that the other system is not functioning) shall be to provide sufficient capacity to assure that (l) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary - not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions - maintained in the event of postulated accidents.

The onsite electric power supplies, including the batteries, and the onsite electric distribution system shall have sufficient independence, redundancy, and testability to perform their safety functions, assuming a single failure.

Electric power from the transmission network to the onsite electric distribution system shall supplied by two physically independent circuits (not necessarily on separate rights of way) designed and located so as to minimize, to the extent practical, the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions. A switchyard common to both circuits is acceptable. Each of this circuits shall be designed to be available in sufficient time, following a loss of ail onsite alternating current power supplies and other offsite electric power circuit, to assure that specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary - not exceeded. One of these circuits shall be design to be available within a few seconds following a loss of coolant accident to assure that core cooling, containment integrity, and other vital safety functions - maintained.

Provisions shall be included to minimize the probability of losing electric power from any of the remaining supplies as a result of, or coincident with, the loss of power generated by the nuclear power eluate, the loss of power from the transmission network, or the loss of power from the onsite electric power supplies.

General Design Criterion 18 - Inspection and Testing of Electric Power System

Electric power system important to safety shall be designed to permit appropriate periodic inspection and testing of important -as and features, such as wiring, insulation, connections, and switchboards, to assess the continuity of the systems and the conditions of their components. The system shall be designed with a capability to test periodically (l) the operability and functional performance of the components of the system, such as onsite power sources, relays, switches, and buses, and (2) the operability of the system as a whole ad, under conditions as close to design as practical, the full operation sequence that brings the systems into operation, including operation of applicable portions of the protection system, and the transfer of power among the nuclear power unit, the offsite power system, and the onsite power system.

General Design Criterion 21 - Protection Reliability and Testability

The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (I) no single failure results in the loss of the protection function and (2) removal from service of any component or channel does not result in the loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determined failures and losses of redundancy that may have occurred.

10 CFR 50.63 - Loss of All Alternating Current Power

This section provides requirements that light-water-led nuclear power plants must be able to withstand for a k specified duration and recover from a station blackout. It specifies that an alternate ac power source will constitute acceptable capability to withstand station blackout provided an analysis is performed which demonstrates that the plant has this capability from the onset of the station blackout until the alternate ac source(s) and required shutdown equipment - started and lined up to operate.

INSAG-3 Principle: 4.2.3.12 Control of accidents within the design basis

> *Provisions are made at the design stage for the control of accidents within the design basis, including the specification of information and instrumentation needed by the plant staff for following and intervening in the course of accidents.*

Relevant US NRC Requirements:

Criterion 13 - Instrumentation and Control

Instrumentation shall be provided to monitor variables and system over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and system that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated system. Appropriate controls shall he provided to maintain these variables and system within prescribed operating ranges.

Criterion 20 - Protection System Functions

The protection system shall he designed (1) to initiate automatically the operation of appropriate system, including the reactivity control system, to assure that specified acceptable fuel design limits - not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of system and components important to safety.

Criterion 29 - Protection Against Anticipated Operational Occurrences

The protection and reactivity control system shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.

Next page(s) left blank

Part III
PLANT DESIGN INFORMATION PAPERS PRESENTED AT THE TCM

BASIC INFORMATION ON DESIGN FEATURES OF THE V-392 ADVANCED REACTOR PLANT

B. VOLKOV, V. FEDOROV, M. ROGOV, G. BIRYUKOV,
A. PODSHIBYAKIN, V. NOVAK, N. FIL
Gidropress EDO,
Podolsk

V. NOVIKOV, V. IGNATYEV
Kurchatov RSC,
Moscow

Russian Federation

Abstract

The paper describes the V-392 (also known as VVER-88) advanced reactor plant concept which represents an evolution of the design of the VVER-1000 nuclear power plants of model V-320 currently operating in the Russian Federation and other countries. The paper consists of three parts: - a brief description of the plant concept; - a description of how the plant compares with the safety principles of INSAG-3 for 15 selected design areas; and - an extended data list. The concept description outlines the main elements of the safety philosophy, describes the main features of the reactor plant and its safety systems, and provides a list of main operational occurrences and design accidents, as well as beyond-design accidents. The second part discusses plant performance in the areas of: - plant process control systems; - automatic safety systems; - protection against power transient accidents; - reactor core integrity; - automatic shutdown systems; - normal heat removal; - emergency heat removal; - reactor coolant system integrity; - confinement of radioactive material; - protection of confinement structure; - monitoring of plant safety status; - preservation of control capability; - station blackout; - control of accidents within the design basis; and - mitigation and control of severe accidents. The third part, finally, presents data related to the power plant as a whole, data on reactor core and fuel, on the reactor coolant system, the reactor pressure vessel, coolant pumps, steam generators and pressurizer, and on the containment.

1. BRIEF DESCRIPTION OF THE CONCEPT

1.1. The main elements of the safety philosophy

The principle of ensuring the safety of the personnel, the population and the environment against radiation effects exceeding the prescribed radiation doses is used as the basis for design. This principle also addresses the standards for releases of radioactive substances and their content in the environment under normal operation conditions, anticipated operational occurrences, and in design and beyond-design-basis accidents during the plant service life.

The objective of the design of the reactor plant and of the nuclear plant process systems was to achieve that the estimated probability of a severe fuel damage does not exceed 1.0E-6 per reactor-year and that the probability of accidental radioactive releases, as prescribed by regulatory requirements, does not exceed 1.0E-7 per reactor-year.

NPP safety is achieved by consistent implementation of the principle of "defence-in-depth" based on the application of a system of barriers on the path of spreading ionizing radiation and radioactive substances into the environment, as well as on a system of engineered safeguards and organizational provisions for protection of these barriers.

A consistent implementation of the "defence-in-depth" principle is provided with the following:

- installation of successive physical barriers on the path of spreading radioactive substances: fuel matrix, fuel element cladding, primary circuit boundary, containment;
- taking into account postulated initial events that could lead to a loss of efficiency of those barriers;
- determination, for each postulated event, of design measures and actions of operating personnel required to keep the integrity of the barriers mentioned, and mitigation of consequences of damage to such barriers;
- minimization of the probability of accidents resulting in an escape of radioactive substances;
- consideration of beyond design basis accident management.

The principal technical decisions have been supported by the operational experience of more than 90 reactor-years of VVER-1000-type NPPs.

The design is developed in accordance with the last versions of the Safety Regulations for NPP /1/, /2/ by three organizations: OKB "Gidropress", Russian National Research Centre "Kurchatov Institute" and LOAEP, all being well known designers of VVER NPP. IAEA QA requirements and international standards ISO 9000 are taken into account in the design.

In the plant safety concept, modern worldwide trends in NPP safety improvements are considered in order to meet the normative requirements for NPP safety, which are constantly becoming more strict, for as long a period as possible.

The principal features that largely determine nuclear plant safety are as follows:

- possibility of subcriticality provision with solid control rods at any moment of the plant life under a coolant temperature decrease to 120°C;
- application of horizontal steam generators with a large water inventory and with better conditions for natural circulation in the primary circuit in comparison with vertical steam generators;
- application of an emergency core cooling system, based on the principles of both passive and active operation, that provides for the possibility of long-term residual heat removal after accidents with primary leaks accompanied by a station blackout;
- application of a system of passive residual heat removal from the reactor plant in case of a station blackout and loss of emergency power supplies for 24 hours;
- application of a passive core flooding system;
- application of a quick boron supply system;
- application of a double wall concrete containment;
- application of a diagnosis system for the equipment of the systems important to safety for periodical inspection during shutdown, and for on-line diagnosis during reactor operation;

- application of an automatic control system of improved reliability with self-diagnosis, and of an expert system giving advice to the operator;
- application of an emergency system for discharging and purification of radioactive materials of the steam-gas mixture vented from the containment if the pressure exceeds the allowable values in beyond design basis accidents.

1.2. Description of the reactor plant and plant safety systems

1.2.1. General characteristics

The reactor plant includes a reactor coolant system, a primary pressure control system and a primary overpressure protection system. The reactor coolant system consists of 4 loops, with a horizontal steam generator and a reactor coolant pump in each. A schematic drawing of the reactor building is shown in Fig.1.

1.2.2. Reactor

A schematic drawing of the reactor is shown in Fig.2. The reactor vessel is similar to that of a serial VVER-1000 reactor. The core consists of 163 fuel assemblies. 121 control clusters can be used in the reactor emergency protection system. Pitch electromagnetic drives with position indicators are used as driving devices for the control clusters. The drives are installed on the reactor top head.

The effective operation time between refuelling is 7000 effective hours. The average burnup of the fuel unloaded is up to 43 MW days/kg. The number of fresh assemblies loaded during annual refuelling is 54.

1.2.3. Reactor coolant pump

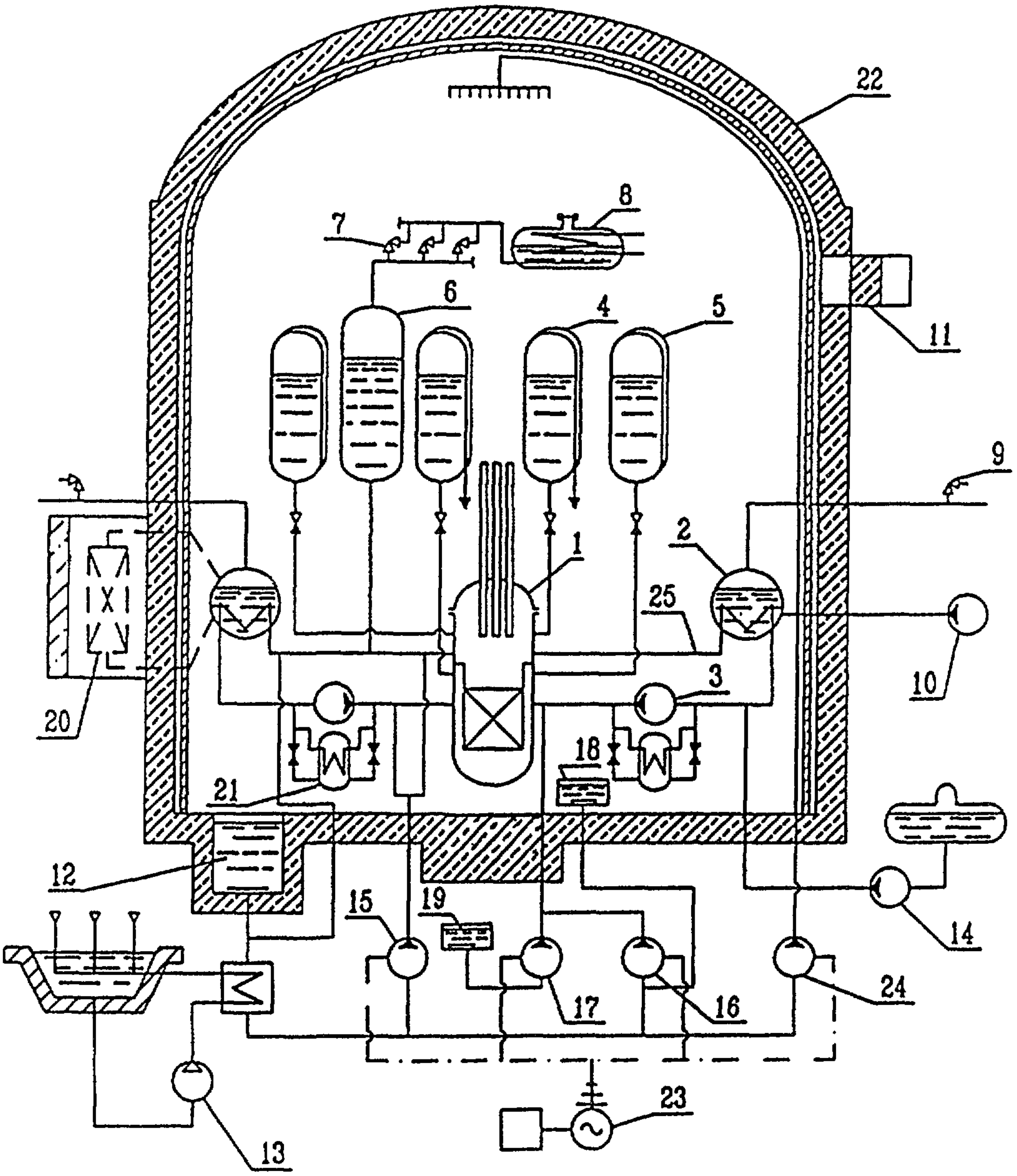
The reactor coolant pump (RCP) is a vertical, one-stage, centrifugal pump with an autonomous lubrication system housed in a spherical case. The RCP subsystems prevent the escape of radioactive coolant out of the primary system. The electrical motor is of the vertical type, three-phase, and has two velocities. A non-combustible lubricant is used in the electrical motor. A drawing of the RCP is shown in Fig.3.

1.2.4. Steam generator

The steam generator (SG) is of the horizontal, one-vessel type, with an immersed heat exchange area consisting of tube bundles horizontally arranged. The SG is a modernization of the standard SG PGV-1000. The positive experience of operating VVER-1000 and VVER-440 SGs have been taken into account. In particular, the perforated part of the primary collector is made of stainless steel 0KH18N10T that has shown good properties during the operation of the VVER-440 SG primary collectors. For internals inspection, hatches of 500 mm diameter on the elliptic bottom, as well as hatches of 1000 mm diameter in the cylindrical part of the steam generator, are provided. A schematic drawing of the steam generator is shown in Fig.4.

1.2.5. Pressurizer

For the V-392 plant it is anticipated to use the pressurizer applied in the standard VVER-1000 design. A schematic drawing of the pressurizer is shown in Fig.5.



1	Reactor
2	Steam generator
3	Main pump
4	6.0 MPa ECCS accumulator
5	1.2 MPa ECCS accumulator
6	Pressurizer
7	Pressurizer safety valve
8	Bubbler
9	SG safety valve
10	SG emergency feedwater pump
11	Filter
12	Boron solution store
13	Service water pump
14	Primary make-up pump
15	ECCS LP pump
16	ECCS HP pump
17	ECCS HP pump
18	Boron solution
19	Boron solution
20	Passive residual heat removal system
21	Rapid boron introduction system
22	Double containment
23	Diesel-generator
24	Springler pump
25	Main pipe

Fig. 1. The V-392 RP safety system concept

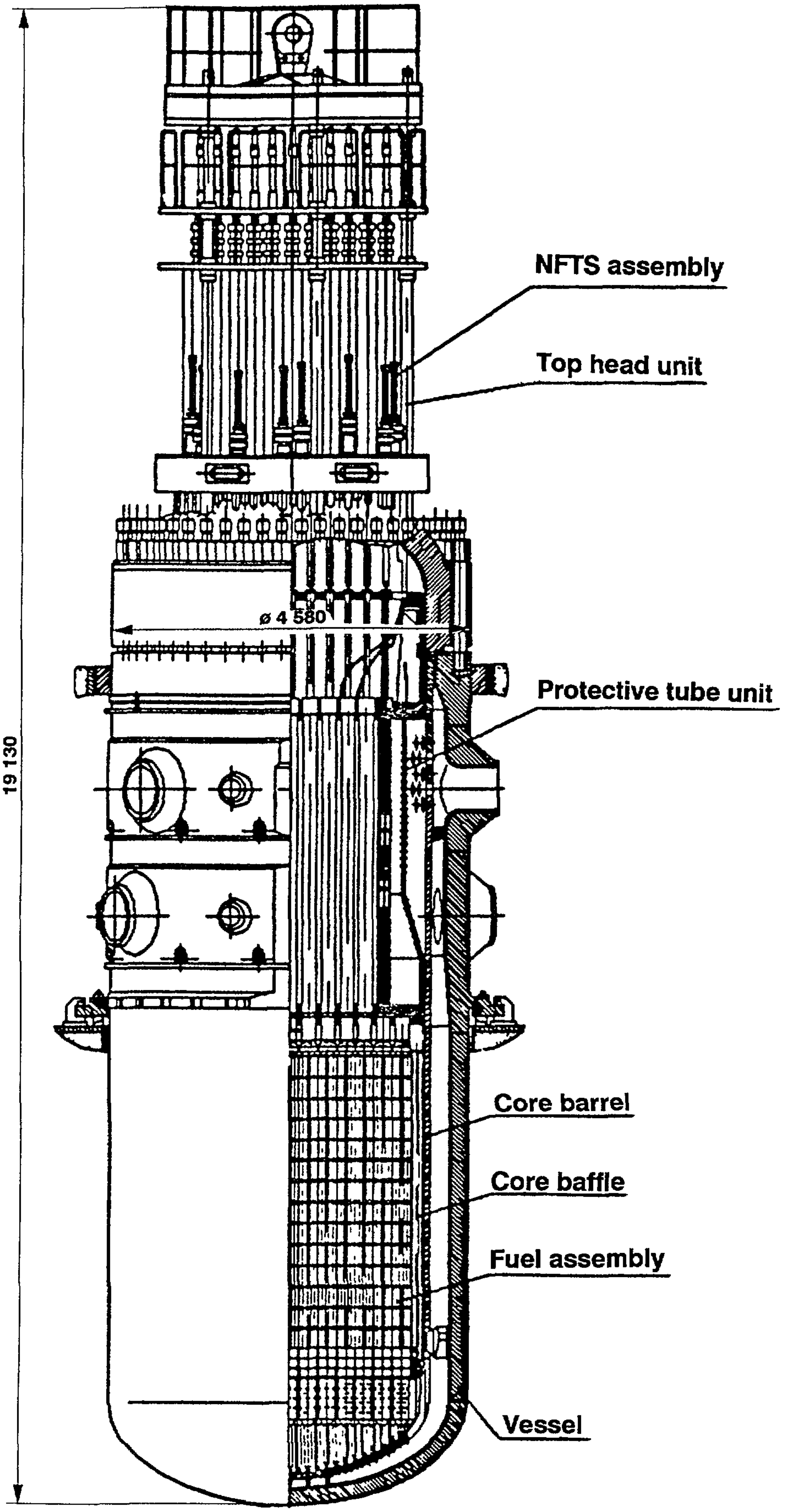


Fig. 2. Reactor

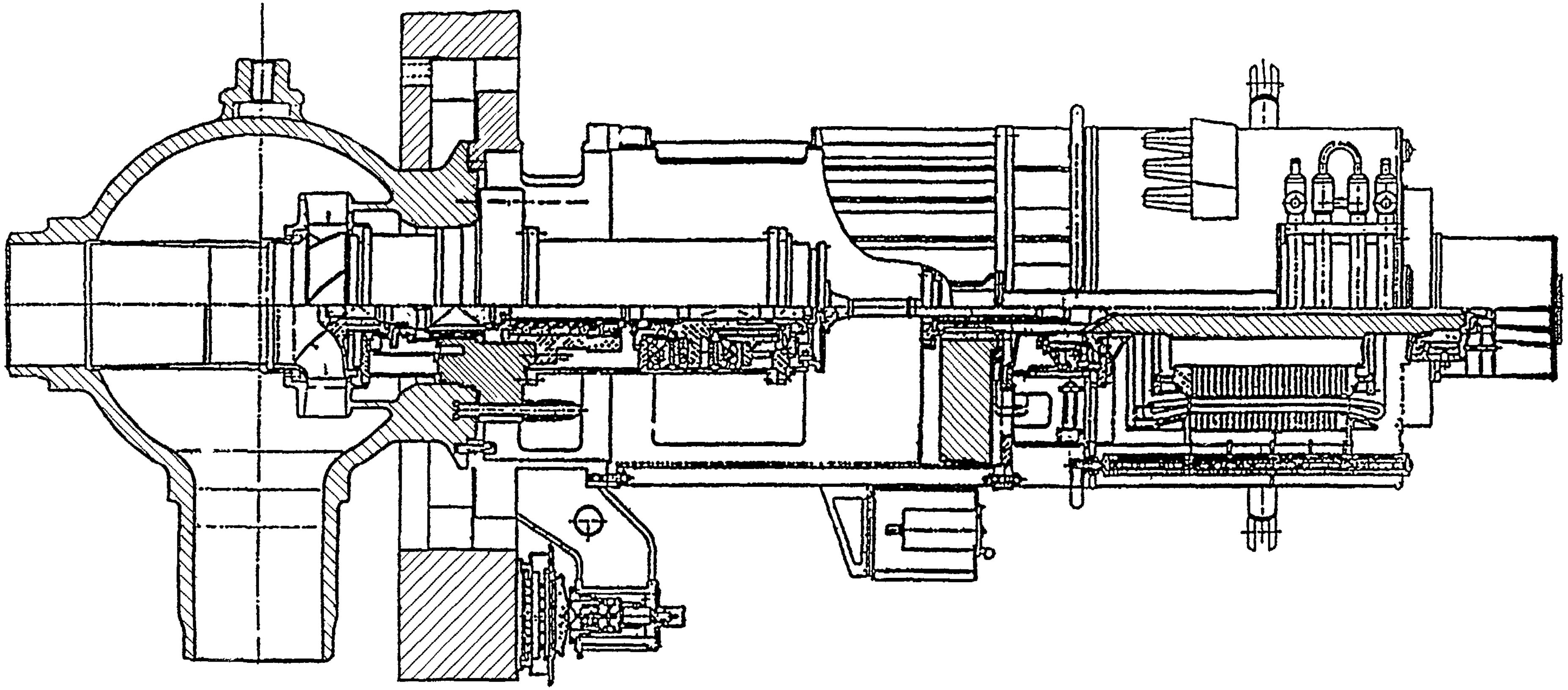
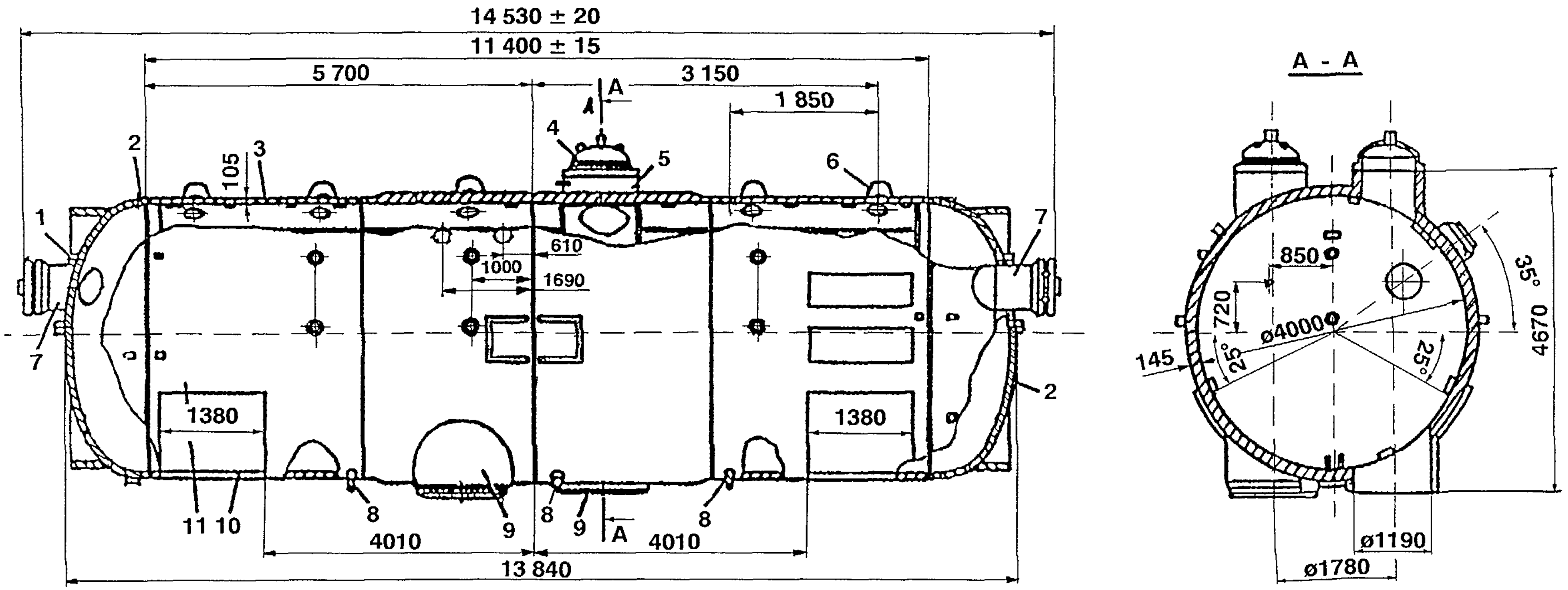


Fig. 3. Main coolant pump



1 Sleeve width Dnom 20

2 End plate

3 Shell

4 Top plate

5 Nozzle width Dnom 800

6 Nozzle width Dnom 350

7 Nozzle width Dnom 500

8 Periodic blowdown nozzle

9 Nozzle width Dnom 1200

10 Support plate

11 Strap

Fig. 4. Steam generator

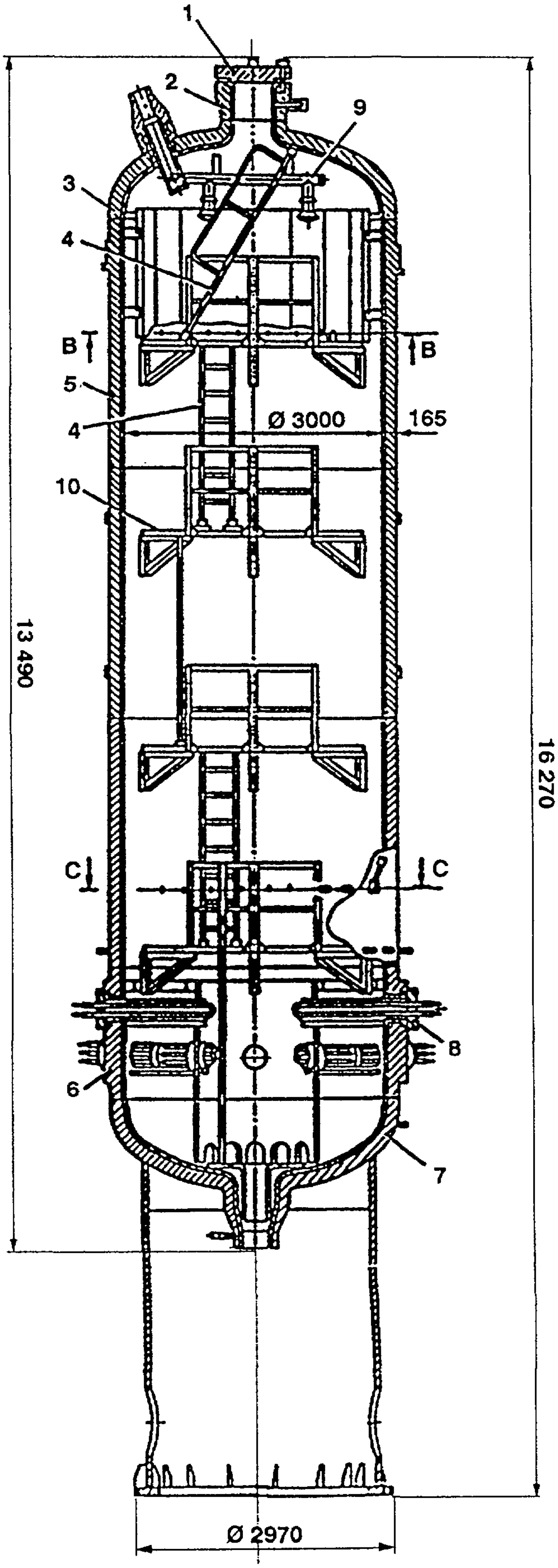


Fig. 5. Pressurizer

1.2.6. Emergency core cooling system

In the design, an emergency core cooling system (ECCS) is applied which consists of two parts, one based on a passive principle of operation and the other based on an active one.

The ECCS provides for a possibility of long-term residual heat removal in case of primary leak accidents accompanied by a station blackout. At the first stage of the accident, the hydrotanks with nitrogen under pressure are in operation. After these are emptied, the active part of the system begins to operate.

The active part of the ECCS includes two independent trains having an overall redundancy within each train. Each of the 4 subtrains thus formed is capable to fulfill the necessary system functions. A subtrain includes the sump of the containment, a high pressure injection (HPI) pump, a jet pump installed on the discharge side of the HPI pump, an emergency cooling-down heat exchanger and pipelines and fittings. The emergency power supply of each subtrain is provided from the related diesel generator.

1.2.7. System of passive residual heat removal from the reactor plant

A system of passive residual heat removal from the reactor plant is used (PHRS) in the design. The design basis of the PHRS is that in case of a station blackout, including loss of emergency power supply, the removal of residual heat should be provided without damage of the reactor core and the primary system boundary 24 hours. Part of the PHRS is an air-cooled heat exchanger that is installed outside of the containment. The heat exchanger is connected to the SG secondary side in a way that the steam from the steam generator is condensed in the heat exchanger giving its heat to the atmospheric air. The condensate generated is returned into the steam generator. The cooled medium motion occurs owing to natural circulation.

1.2.8. Core passive flooding system

The core passive flooding system includes 4 groups of hydrotanks under atmospheric pressure which are coupled with the pipelines connecting the ECCS hydroaccumulators with the reactor (see 1.2.6). The hydrotanks of the passive core flooding system are connected to the primary system at 1.5 MPa and allow to flood the core under the hydrostatic pressure of the water column, and to remove the reactor residual heat during the last stage of a LOCA for at least 12 hours.

1.2.9. Quick boron supply system

The quick boron supply system (QBSS), being developed as an additional reactor trip system, comprises a system of 4 special loops bypassing the main coolant pumps. Each loop consists of a hydro-accumulator containing concentrated boron acid solution, and of pipelines with quick-acting valves that do not require electric power for their opening. In fact, this system, being a part of the primary circulating circuit, allows to consider a reactor plant with such a system as a plant with increased inherent safety.

1.3. List of the main operational occurrences and design accidents

Below a list is presented of the main groups and of the names of the most important conditions which are considered in the design in the two categories of anticipated operational occurrences and accident conditions.

1.3.1. Anticipated operational occurrences

Reactivity-induced occurrences

- Uncontrolled withdrawal of a control rod bank
- Boron concentration decrease in primary coolant

Occurrences with a reduction of the primary coolant flow rate

- Disconnection of several or all RCPs
- Loss of NPP unit electric power supply

Occurrences with a loss of secondary coolant

- Inadvertent opening of a steam dump valve or a SG safety valve with subsequent failure to close

Conditions with variation of steam generator steam load or feed water flow rate

- Steam load change of steam generators
- Inadvertent closure of a quick-acting isolation valve in a steam line
- Inadvertent connection of the system of passive residual heat removal from the reactor plant

Abnormal operation of the primary system

- Inadvertent operation of the pressurizer spray system

Abnormal operation of fuel

- Improper fuel loading and operation of fuel assemblies in wrong positions

1.3.2. Design accidents

Reactivity-induced accidents

- Control rod ejection as a consequence of a control rod drive casing break
- Loop start-up operator fault

Loss of primary coolant accidents

- Inadvertent opening and subsequent erroneous non-closure of a pressurizer safety valve
- Small leaks with loss of coolant as a result of postulated breaks of primary pipelines of diameter less than 100 mm
- Large leaks with loss of coolant as a result of postulated breaks of primary pipelines of diameter greater than 100 mm, up to the diameter of a main coolant pipeline

Loss of secondary coolant accidents

- Break of SG feedwater line
- Spectrum of steamline breaks within and outside the boundaries of the containment (including the case with a simultaneous break of a heat exchanger tube in the SG with the injured steamline)

Primary coolant flow rate reduction accidents

- Instantaneous seizure or break of a RCP shaft

Primary to secondary leak accidents

- SG tube rupture
- SG primary collector cover break-off
- Leak of SG primary collector

Accident situations with fuel

- Fuel handling accidents
- Drop of a fuel assembly during refuelling
- Gaseous radioactive waste containing system leak or damage
- Compensable leak of the spent fuel storage pond liner
- Drop of loads into the reactor and into the spent fuel storage pond

Fire in NPP compartments related to safety assurance

1.4 Main beyond-design accidents

1.4.1. Anticipated occurrences and design accidents accompanied by loss of NPP alternate power supply for 8 and 24 hours.

1.4.2. Failure of the reactor control and protection system to operate under operational occurrences and design accidents

2. DESCRIPTION OF 15 SPECIFIC DESIGN AREAS AS SELECTED FROM INSAG-3

In the following sections the reference to INSAG-3 is put in parentheses after each heading.

2.1. Plant process control systems (4.2.2.1)

The reactor plant control system secures fulfillment of the following main functions:

- monitoring of the unit operation, radiological situation, state of equipment and systems in all conditions;
- remote control;
- automatic control of reactor plant, secondary circuit and auxiliary systems parameters;
- process protection and interlocking;
- emergency and preventive protection of the reactor.

The following priority of control commands (in the order of priority diminishing) is secured in the control system of the reactor plant:

- emergency and preventive reactor protection and control of safety systems;
- process protection and interlocking;
- manual remote control;
- automatic control (the main controlled parameters are: neutron flux in the core, primary pressure, secondary pressure, water levels in steam generators and the pressurizer);
- recording and archiving of the main parameters under normal and emergency conditions.

Under emergency conditions the main parameters and the equipment status are continuously recorded.

2.2. Automatic safety systems (4.2.2.2)

The following systems belong to the class of automatic safety systems:

- primary overpressure protection system
- emergency core cooling system
- system of passive heat removal from the reactor plant
- passive hydrostatic core flooding system
- system of quick-acting isolation valves in steamlines
- secondary overpressure protection system
- quick-acting boron supply system
- emergency diesel-generators
- emergency system of reliable direct and alternate electric current power supply

Reactor emergency protection system

The reactor emergency protection system provides reliable disconnection of electric power supply and, as a consequence, a drop of emergency protection rods into the core. In this case, disappearance of signal of original cause does not stop the initial action of the emergency protection (see 2.5 for more detail).

Primary overpressure protection system

The system comprises three safety valves for discharging steam or a steam-water mixture from the pressurizer if its pressure increases above the permissible one, as well as a subsystem for receiving a steam-water mixture. This subsystem involves a bubbler and pipelines connecting it to the outlets of the safety valves.

Emergency core cooling system

The emergency core cooling system (ECCS) involves the following complex of subsystems:

- a subsystem of hydrotanks with nitrogen under pressure
- a subsystem of high pressure injection pumps

The energy supply for the active elements of the system is provided by the reliable emergency electric power supply system. Each of the four subtrains of the system has its own subtrain of reliable electric power supply, including a diesel-generator.

System of passive heat removal from the reactor plant

The passive heat removal system (PHRS) is intended for removing the residual reactor power during a station blackout for 24 hours. The PHRS consists of four independent trains, each of them connected via the steam generator to the respective loop of the reactor plant. Each train has pipelines for steam supply and removal of condensate, valves, and a heat exchanger outside the containment in which the steam generated in the steam generators due to the heat released in the reactor condenses and rejects its heat to the ambient air.

Passive core flooding system

The core passive flooding system includes four groups of hydrotanks under atmospheric pressure which are coupled with the pipelines connecting the ECCS hydroaccumulators with the reactor. The hydrotanks of the passive core flooding system are connected with the primary system at 1.5 MPa. They allow to flood the core due to the hydrostatic pressure of the water column, and to remove the reactor residual heat in the last stage of a LOCA for at least 12 hours.

Secondary overpressure protection system

The secondary overpressure protection system is intended for preventing the secondary pressure to increase above the permissible value. The system incorporates quick-acting steam dumping valves and steam generator safety valves.

System of quick-acting isolation valves in steamlines

Quick-acting isolation valves in steamlines close at:

- increase of level in the SGs above the permissible one;
- increase of radioactivity in the SGs above the permissible one, on the appearance of signals of a steamline rupture.

They are intended, respectively, for the protection of the turbine from steam of high humidity, for preventing radioactivity releases from the SGs, and for restricting the steam blow down after a rupture of the secondary circuit.

Quick boron supply system

The quick boron supply system (QBSS), being an additional reactor trip system, comprises a system of four special loops bypassing the main coolant pumps. In the system, there are a hydroaccumulator containing concentrated boron acid solution and pipelines with quick-acting valves that do not require electric power supply for their opening. Those valves open during occurrences and accidents with failure of scram, and concentrated boron solution is pressed out of the hydroaccumulators into the primary loops, and further into the reactor. In case of a station blackout the boron solution delivery occurs in the period of main coolant pump (MCP) coast-down. A considerable MCP flywheel inertia provides the possibility of ejecting all boron concentrate from the QBSS hydroaccumulators. The amount and concentration of the boron solution are chosen to provide a definite equivalency from the viewpoint of reactivity inserted by this system and by the solid absorber scram.

Diesel generators

The diesel generators provide the power supply to safety related systems for 2 days using the internal fuel stock, and for unlimited time if fuel is provided from the outside.

System of reliable direct current power supply

The system of reliable direct current power supply consists of storage batteries. It provides power to the electromagnetic circuits for actuating the automatic safety systems as well as for recording necessary plant parameters during 24 hours.

2.3. Protection against power transient accidents (4.2.3.1)

Protection against transients due to the introduction of reactivity is secured by the operation of the emergency protection in response to a signal of reaching the set neutron flux or in response to a signal of reaching the setting of reactor period decrease.

2.4. Reactor core integrity (4.2.3.2)

2.4.1. Permissible limits of fuel cladding damage

The operating limits of fuel cladding damage allow under normal conditions 0,2% of the fuel elements (rods) to have gas leakiness flaws, and 0,02% of the fuel elements (rods) to have direct fuel-coolant contact. The corresponding safe operation limits for anticipated events are: 1% of fuel elements with gas leakiness flaws, and 0,1% of rods with direct fuel-coolant contact.

Maximum design limits specify that the following conditions should not be exceeded:

- 1200°C fuel rod cladding temperature;
- fuel rod cladding local oxidation depth is not more than 18% of initial cladding thickness;
- reacted zirconium mass fraction is not more than 1% of initial fuel rod cladding mass.

In addition, the threshold power generation leading to fuel rod destruction should not be exceeded, and fuel melting should be excluded in design basis accidents associated with a rapid positive reactivity insertion.

2.4.2. Under design conditions the following mechanical requirements are ensured:

- retention of the required geometry and position of the fuel elements in the fuel assembly, and of the fuel assembly in the core;
- necessary margin of axial or radial expansion of a fuel element, taking into account the variation of sizes as a result of temperature and radiation effects, of pressure differences, and of interaction between fuel pellets and fuel cladding;
- provision of the structure for the fuel system to be able to withstand all mechanical loads under design conditions;
- provision of adequate coolant flow taking into account vibration, pressure differentials, pressure pulsation, and flow instability;
- provision of normal movement of control rods and of emergency protection under design conditions.

2.4.3. Fuel assembly design features (see also section 3)

- triangular lattice of fuel assembly;
- high ratio of heat exchange surface to fuel element volume;
- relative thickness of fuel element cladding such as to permit the allowable degree of interaction between fuel and cladding during a burnup up to 52 MWd/kg, and to avoid exceeding the permissible level of coolant radio-activity.

2.5. Automatic shutdown systems (4.2.3.3)

The solid rods of the emergency protection actuate in response to the following signals:

- decrease of reactor period
- increase of neutron flux
- decrease of margin to saturation temperature in any hot leg
- increase of coolant temperature in any hot leg
- decrease of pressure differential over the primary coolant pumps
- de-energization of several primary coolant pumps
- decrease of pressure in the reactor
- increase of pressure in the reactor
- increase of pressure in a SG
- decrease of pressure in a SG coinciding with a definite increase of the primary and secondary saturation temperature difference
- decrease of water level in a SG
- increase of pressure in the containment

The parameters chosen permit to secure the necessary reduction of reactor power for meeting the design criteria under all design conditions. Automatic disconnection of power governors, and interlocking of all operator's actions on control rods occur when the emergency protection operates.

Two sets of instrumentation are provided, generating the commands for the emergency protection and operating in parallel using an "or" logic. The signals for operation of the emergency protection are generated using a "2 out of 3" majority logic in any set.

However, with the aim of enhancing of NPP safety, failure of the emergency protection system of the reactor is postulated in some beyond design basis accidents by considering scram failure under operational occurrences and in design accidents.

2.6. Normal heat removal (4.2.3.4)

Normal heat removal is secured by coolant circulation in the primary circuit, steam generation in the SGs, transfer of steam energy to the turbogenerator, and condensation of the spent steam in the turbogenerator condenser.

Scheduled cool-down is carried out at the rate of 30°C/h. Duration of the process is 16 hours. It proceeds in the following way:

- reactor shutdown
- increase of boron concentration to the standby value
- steam/water cool-down
- water-to-water cool-down to a primary temperature less than 130-150°C.

The same systems alongside with the emergency systems take part in heat removal from the reactor under operational occurrences and in design accidents, excluding the turbogenerator, after reaching the respective settings and its disconnection.

In the design, necessary measures are taken for using normal heat removal systems alongside with emergency ones under beyond-design accidents for mitigating the consequences of these accidents and for NPP safety assurance.

2.7. Emergency heat removal (4.2.3.5)

The most typical condition without loss of primary coolant, giving the highest requirements for the emergency heat removal system, is a station blackout. In this case, heat removal from the reactor is performed due to natural coolant circulation in the primary circuit. A system of passive residual heat removal provides emergency heat removal from the steam generators at 2% of reactor rated power.

In the case of accidents with loss of integrity of the primary circuit, emergency heat removal is performed by the emergency core cooling system and, if necessary, by the passive core flooding system.

2.8. Reactor coolant system integrity

2.8.1. General

Integrity of reactor coolant pressure boundary is provided owing to appropriate design and inspection during manufacture, installation and operation. The integrity of the primary circuit is provided by limiting pressure and temperature of the primary coolant, respectively, to below 1,1 of the design pressure, and to below the design temperature under all design conditions.

All components of the primary circuit that experience temperature stresses are subject to strength analysis, and are designed with due regard for the results of this analysis.

2.8.2. Primary overpressure protection

Overpressure protection in the primary circuit is provided by the primary overpressure protection system. The capacity of this system prevents exceeding the allowable pressure in the primary circuit under all design conditions.

Reliability of system operation is provided owing to system compliance with the requirements of the normative documentation, to a choice of a supplier of high skill and competence, and to quality control at all stages of manufacture, installation, pre-operational tests and during operation.

2.8.3. Inspection and tests of the primary pressure boundaries

Inspection of the equipment state during operation provides timely detection of defects by:

- measurement of the parameters by deviation of which from the normal values the soundness of individual components of the system is determined;
- check of the metal state during periodical inspections.

Pre-operational, periodical in-service, and extraordinary tests of the primary pressure boundaries are performed. Extraordinary testing is done:

- after an earthquake exceeding the operating basis earthquake;
- after accidents which cause variation of operating parameters of the equipment or pipelines exceeding design values.

Fulfillment of necessary requirements for provision of accessibility either for direct or remote inspection of metal and welds is provided.

2.8.4. Determination of leaks through the primary circuit boundary in the steam generator

Check of leaks is performed by means of comparison of the primary and secondary coolant radioactivity. The check is performed with J-131, J-135, Na-24, K-42 as reference isotopes. The determination of specific radioactivity of let-down water of each steam generator by testing dry residue is performed once in a shift.

2.8.5. Concept of endurance of reactor vessel integrity

All materials used for the manufacture of the vessel are qualified and corroborated by the experience of long-duration operation (90 reactor-years). For the manufacture of the main components of the vessel and the top head ingots are produced which are then forged into shrouds and plates. All components of the vessel and the top head are one-piece-solid-forged. The vessel bottom and top heads, as well as the nozzles in the vessel shrouds, are manufactured by die-stamp technique.

During manufacture, the reactor vessel is subject to inspection in line with the requirements of the working documentation for manufacture. Geometrical dimensions and qualitative fulfillment of procedures shall be tested by both destructive and non-destructive methods. The vessel is to inspected during the preoperational tests of the reactor plant. In this process the reactor vessel is subjected to hydraulic and non-destructive tests. Periodic examination of the reactor vessel during operation is performed with the aim of:

- detected defects control;
- detection and fixation of metal defects;
- detection and fixation of variations of physical-mechanical properties and metal structure;
- evaluation of metal state.

All welded joints and vessel cladding are subject to non-destructive tests. Destructive tests are performed by means of testing surveillance specimens.

2.8.6. Materials of the primary pressure boundaries

The primary pipelines, the RCP body, and the steam generator tube bundles are made of austenitic stainless steel. Reactor and pressurizer vessels are made of low-alloyed carbon steel (see section 3). They have a cladding made of austenitic stainless steel.

Compatibility of structural materials of the primary pressure boundary with the primary coolant is provided by maintaining the necessary water chemistry. In the design, fulfillment of the necessary requirements for fracture toughness and brittle critical temperature of ferritic materials is provided. Control of variation of mechanical properties, the rate of growth of defects, and a shift of brittle critical temperature of the reactor vessel metal is performed on the surveillance specimens irradiated in the reactor in areas of the highest neutron flux. Base metal cuts out of the allowance in the core shroud and of the weld are used as surveillance specimens.

2.9. Confinement of radioactive material (4.2.3.7)

2.9.1 Confinement of radioactive material during normal conditions and operational occurrences is provided by keeping the integrity of all barriers: fuel matrix, fuel element cladding, primary pressure boundary, and containment.

2.9.2 Confinement of radioactive material in design accidents is provided by maintaining containment integrity.

2.9.3 Control and confinement of radioactive material in design accidents with a leak from the primary to the secondary circuit is provided by isolation of the affected steam generator on both the steam and water sides with the help of quick-acting shut-off valves. These are actuated by a signal of radioactivity increase in the injured steam generator.

2.9.4 Confinement of radioactive material in beyond-design accidents is provided by the concrete structures of the base of the containment and by operation, if necessary, of the filtration plant for controlled removal of medium from the containment.

2.10. Protection of confinement structure (4.2.3.8)

A double wall containment is provided in the design. The inner shell bears the loads arising from a sequence of internal accidents. The outer shell provides protection from external loads (as tornado, hurricane, shock wave, plane crash etc.).

2.10.1. Loads acting upon the outer protective shell of the containment

The design is performed taking into account two levels of seismicity: the operating basis earthquake (OBE) of magnitude 7 on the MSK-64 scale and the safe-shutdown-earthquake (SSE) of magnitude 8 on the MSK-64 scale.

The reactor plant equipment is calculated for seismic effects proceeding from the following conditions. During an operating basis earthquake normal operation of the reactor plant is to be provided. During a safe-shutdown-earthquake reactor shutdown and reactor plant shutdown cooling are to be provided.

All civil structures, process and electrotechnical equipment, pipelines, instrumentation and so on are divided into 3 seismic categories depending upon the degree of responsibility for safety ensurance during seismic effects and for serviceability after an earthquake. Components and systems being related to seismic category 1 (the highest) shall fulfill their functions concerning NPP safety ensurance in the course of an earthquake, and after it, with intensity to SSE inclusive, and at OBE to keep its serviceability. Seismic category systems include:

- systems of normal operation, failure of which during seismic events, SSE inclusive, may result in a release of radioactive material in such quantities that causes excessive population dose in comparison with the specified values;
- safety systems for keeping the reactor in a subcritical state, for emergency heat removal from the reactor, for confinement of radioactive products, and buildings, structures and equipment, mechanical damages of which during seismic events, SSE inclusive, may result in failure of these systems.

The outer protective shell structure is designed for the impact of an environmental shock wave having a front pressure of 0,03 MPa, and a compression phase duration of up to 1 second, and for a crash of a 5,0 tonne plane creating a 1200 ts impulse with an impact duration time equal to 0,1 second and with a contact area equal to 12,0 square meters.

2.10.2. Loads on the inner containment

The inner containment is designed for the following loads:

- impact of the maximum design basis accident conditions with a maximum excess pressure of 0.4 MPa, and a maximum temperature of 150°C;
- impact of missiles and steam-water jets inside the containment.

Under design basis accidents, the localization safety systems provide for confinement of radioactive releases inside the containment and for heat removal from the containment. For beyond design basis accidents, a system for containment pressure venting and a filtered discharge from the containment is provided.

2.11. Monitoring of plant safety status (4.2.3.9)

2.11.1. Monitoring and identification of NPP safety status

The monitoring and control system provides an automated diagnosis of the state and the operating conditions of the NPP. Monitoring and presentation of information on the reactor coolant system, on the containment, on all the systems important for safety, under all operating conditions of the NPP is provided through remote control. Personnel performs monitoring of the NPP systems as well as of the parameters defining the NPP safety status in accordance with the service manuals from the main control room (MCR). Engineered features of the on-line diagnosis system give a possibility for an operator to evaluate the plant state during an accident and after it.

2.11.2. Facilities and presentation of information important for safety

Facilities for the presentation of information including displays and instrumentation for monitoring safety systems ensure:

- indication of control rod position;
- monitoring of neutron flux during operation and refuelling;
- monitoring of level of radioactive contamination of the ground.

The control concerns the following:

- emergency protection of reactor;
- confining system;

- safety systems;
- process equipment protection system.

2.12. Preservation of control capability (4.2.3.10)

In case of a main control room (MCR) failure, for example during a fire, the reserve control room (RCR) is used to provide:

- reactor shutdown;
- monitoring of subcriticality;
- reactor cool-down;
- putting into operation of confining systems.

Possibility of control of the systems important for safety is retained from RCR. Ensurance of habitability under loss of regular ventilation systems during a safe shutdown earthquake (SSE) and associated fire, or other destructions on the site, is provided for the reserve control room.

Local control panels which do not require interaction with the MCR and the RCR are provided for. Their existence, in a number of cases, is determined by considerations of NPP layout. Access to the RCR is provided by an admittance check system.

2.13. Station blackout (4.2.3.11)

2.13.1. The inner consumer power supply system

The inner consumer power supply system is designed for an electric power supply of consumers providing:

- normal NPP operation;
- a unit changeover to a subcritical safe state and a unit up-keep in this state under normal and accident conditions;
- preservation of intact main equipment in case of loss of normal and reserve power supplies;
- monitoring of fulfillment of the main safety tasks during 24 hours in case of a start failure of all diesel generators.

2.13.2. Consumers of the emergency electric power supply system

All consumers of the emergency electric power supply system that require an obligatory power supply after scram can be divided into two groups:

- the first group comprises consumers of direct and alternate current that do not allow an interruption of power supply for more than some fractions of a second in all conditions including blackout,
- the second group comprises consumers of alternate current that allow power supply interruption for a period of time determined by safety limits.

The consumers that do not require an obligatory power supply after scram can be referred to as a third group.

2.13.3. Three inner consumer power supply subsystems

Three inner consumer power supply subsystems are provided for a NPP unit:

- normal operation power supply system that supplies power to consumers of all three groups;
- power supply subsystem that supplies power to consumers of the second group (the safety systems are referred to the second group consumers);
- power supply subsystem that supplies power to consumers of the first group consumers.

The power supply subsystems of the first and second group consumers are designed as two trains. Each train has an inner redundancy. The power supply of the second group consumers is accomplished from transformers. The diesel generators are connected to the sections from which the transformers are fed. Reserve feeding of these sections is also provisioned from reserve transformers.

For the first group consumers, an interruptable power supply device connected to the storage batteries is provided.

The storage batteries are used as direct current sources for the first group consumers. All batteries are designed for a discharge during 24 hours. The batteries operate in a booster charge mode using a rectifier when alternate power is available.

The unit inner power consumers are normally fed from the main transformers. The diesel generators are always ready to be automatically started. The storage batteries are maintained completely charged. All diesel generators are started in case of loss of power of main and reserve transformers buses for more than 0,9 s. In case of a loss of the main and reserve unit sections, an automated startup of all diesel generators by compressed air occurs in less than 15 s from the moment of startup signal.

A remote diesel generator startup from MCR and RCR by a line independent from the automation system is provided. The complete electric power supply of MCR and RCR is provided from the storage batteries in case of blackout.

2.14. Control of accidents within the design basis (4.2.3.12)

The analysis of design basis accidents has been fulfilled assuming no operator intervention for 30 minutes from the onset of an accident. This approach is adopted in order to exclude possible hasty and erroneous actions of the operating personnel during the first period of an accident. It is supposed that in 30 minutes from onset of an accident the operating personnel succeeds to understand correctly the peculiarities of the accident occurred, and become able to perform actions required in accordance with the appropriate manuals.

Further, in case of a failure of some systems, the operating personnel has a possibility to interfere and to fulfill necessary corrective measures in accordance with appropriate manuals. For accident management, the facilities are used to visualize the following main information:

- accident monitoring;
- indication of control rod position;

- indication of isolating valves position;
- monitoring and check of radiation level and radioactive releases;
- monitoring and check of reactor shutdown system and safety system state.

Systems ensuring automatic recording of parameters during any of the accidents within the design basis are provided. An MCR from which the monitoring and control of the reactor plant and the other process equipment, including safety systems, is carried out for each unit of multi-unit plant. Operating personnel with the purpose of decreasing probability of error should not take part in control of high-speed processes. The main control room has:

- alarm light signalling of protection actuation, accompanied by powerful sound signals;
- light signalling of emergency de-energization of mechanisms, accompanied by sound of medium tone;
- warning of deviation of process parameters.

2.15. Mitigation and control of severe accidents

Operating personnel performs actions in accordance with special manuals directed to returning the plant to a controlled state during which the fission chain reaction is stopped, a continuous cooling of the fuel is established and confinement of radioactive products within the preset boundaries is ensured. In the design, work is under way on substantiation of application of engineered features permitting to prevent corium release from the reactor vessel in the case of postulated core melting.

3. EXTENDED DATA LIST

Station output

Rated thermal power of the reactor	3000 MW
Fuel assembly	
Array	triangle
Number of fuel rods	311
Number of guide tubes for absorber/in core instrumentation	18/1
Full length (without control spider)	4.67 m
Fuel rod	
Length	3.837 m
Outside diameter	9.1 mm
Cladding material	zirconium alloy
Cladding thickness	0.61 mm
Initial internal pressure (He)	2 MPa
Fuel pellet	
Material	UO_2
Density (percentage of theoretical density)	94.5%
Reactor core	
Number of fuel assemblies	163
Active height	3.53 m
Equivalent diameter	3.16 m
Rod cluster control assemblies absorber	B_4C
Number of assemblies	121
Absorber rods per assembly	18
Enrichments	
First core	1.6%, 3%, 4.4%
Reload	4.4%
$(H_20/U0_2)$ volume ratio	2.03
Average fuel burn up	43 MWd/t
Total weight of $U0_2$	74 t

Reactor Coolant System

Design conditions:	
Pressure	17.65 MPa
Temperature	350°C
Operating conditions:	
Pressure at vessel outlet	15.7 MPa
Temperature reactor vessel inlet/outlet	293.9/323.3°C

Hydraulic resistance (without inlet and outlet nozzles)	0.37 MPa
Flow rate	84 800 m^3/h
Heat transfer surface in core	4957 m^2
Average fuel linear rating	166.7 W/cm
Peak fuel linear rating	420 W/cm
Average core voluminal rating	107.5 kW/l

Reactor vessel

Overall height with/without the head	19.1/10.9 m
Inside diameter	4.07 m
Wall thickness (opposite to the core)	190 mm
Inlet/outlet nozzle inside diameter	850 mm
Weight (including head)	417 t
Material (forged rings)	15Kh2NMFA
Design pressure/temp.	17.65/350 MPa/°C
Neutron fluence for service life	3.9 E19 n/cm^2

Reactor coolant pump

Type	centrifugal
Number	4
Design pressure/temp.	17.6/350 MPa/°C
Design flow rate	22000 m^3/h
Pump casing material	stainless steel
Speed	1000/750 rpm
Power at coupling, cold/hot	6700/5000 kW
Weight	120 t
Coast down time	100 s
Pump motor inertia	1.472 t x m^2

Steam generator

Type	horizontal
Number	4
Heat transfer surface	5130 m^2
Number of heat exchanger tubes	9157
Tube dimensions	16 x 1.5
Outside/inside diameter of shell	4.3/4.0 m
Total height	9.5 m
Weight	300 t
Shell and tube sheet material	10GN2MFA/0Kh18N10T
Tube material	08Kh18N10T
Steam pressure at SG outlet	6.27 MPa
Steam output	1470 t/h
Feedwater temperature	220°C
Secondary side medium volume	127 m^3
Steam moisture at outlet from SG	0.2 %

Pressurizer

Total volume	79 m^3
Steam volume; full power/zero power	24/ m^3
Design pressure/temp.	17.65/350 MPa/°C
Heating power of the heaters	2520 kW
Number of heaters	28
Outside/inside diameter	3.3/3 m
Total height	13 m
Material	10GN2MFA
Weight	214 t

Containment

Configuration (single or double)	double
Material	steel/reinforced concrete
Gross volume	60 000 m^3
Pressure (design)	0.5 MPa
Height/diameter(outer)	61.6/53 m
Design leak rate of:	
- inner shell	0.3 % of inner shell volume per 24 h;
- outer shell	15 % of volume between outer and inner shell per 24h

REFERENCES

[1] General safety regulations for nuclear power plants (OPB-88), Gosatomnadzor, USSR, Moscow, Energoatomizdat, 1990.

[2] Nuclear safety rules for reactors of nuclear power plants, PBYA RU AS-89, Moscow, 1990.

Next page(s) left blank

TECHNICAL INFORMATION ON DESIGN FEATURES OF THE ABB COMBUSTION ENGINEERING SYSTEM 80+ STANDARD PLANT DESIGN

S. E. RITTERBUSCH, R. S. LEE
ABB Combustion Engineering,
Windsor, Connecticut,
USA

Abstract

The paper describes the System 80+ standard plant design of ABB Combustion Engineering which represents an evolution of the design of the previous System 80 plants built at Palo Verde in the United States and in the Republic of Korea. The paper consists of three parts: - a conceptual overview of the plant design; - a description of how the plant compares with the safety principles of INSAG-3 for 15 selected design areas; and - an extended data list. The conceptual overview outlines the main elements of the safety philosophy, describes the main features of the reactor plant and its safety systems, and provides a list of design accidents, and discusses severe (beyond-design) accidents. The second part discusses plant performance in the areas of: - plant process control systems; - automatic safety systems; - protection against power transient accidents; - reactor core integrity; - automatic shutdown systems; - normal heat removal; - emergency heat removal; - reactor coolant system integrity; - confinement of radioactive material; - protection of confinement structure; - monitoring of plant safety status; - preservation of control capability; - station blackout; - control of accidents within the design basis; and - mitigation and control of severe accidents. The third part, finally, presents data related to the power plant as a whole, data on reactor core and fuel, on the reactor coolant system, the reactor pressure vessel, coolant pumps, steam generators and pressurizer, on the containment, on the turbine, the turbine condenser and generator, and on the main transformer.

1. SYSTEM 80+ CONCEPTUAL OVERVIEW

1.1. Safety philosophy - the main elements

Improved safety is a principal tenet of the System 80+ Standard Plant Design. To improve safety, the design incorporates a balanced measure of design margin, accident prevention, and accident mitigation. As a result, the probability of core damage for the System 80+ design has been reduced by more than two orders of magnitude from current plants. The design also significantly reduces the consequences associated with severe accidents in the unlikely event one should occur.

To produce a safe and simpler design with greater reliability and enhanced operability, the design followed four sets of requirements and policies: (1) the Electric Power Research Institute (EPRI) Advanced Light Water Reactor (ALWR) Utility Requirements Document (URD), which specifies characteristics desired by utilities in future plant designs; (2) the U.S. Nuclear Regulatory Commission (NRC) Severe Accident Policy, which identifies new safety standards to be applied to future nuclear plant designs; (3) the Code of Federal Regulations, Title 10, Part 52 (10 CFR 52), which provides the framework for licensing of new standardized designs; and (4) current NRC regulations, supplemented by emerging policy issues, which are summarized in SECY-93087.

The System 80+ Standard Plant Design meets the stringent design goals in the EPRI ALWR URD Volumes I and II. Specifically, the design complies with the EPRI goals of simplicity, improved reliability, improved accident prevention and mitigation, improved economics, and better man-machine interfaces. Since the design represents an evolutionary advancement over current light water reactor designs, unknown features that could slow the licensing process and/or construction have been avoided. Accordingly, the design does not require prototype testing.

The System 80+ design also complies with the procedural requirements and criteria of NRC regulations including the Three Mile Island requirements codified in 10 CFR 50. In addition, the design addresses all applicable Unresolved Safety Issues (USIs) and the medium- and high-priority Generic Safety Issues (GSIs). Finally, a Probabilistic Risk Assessment (PRA) has been carried out for the design. The PRA was used as a guiding tool during the design process to produce a more robust design that minimizes the potential for core damage and moderates the severity of a severe accident should one occur. Accordingly, the design meets the NRC Severe Accident Policy.

As required by 10 CFR 52, the scope of the System 80+ Standard Plant Design covers an essentially complete nuclear power plant and includes all structures, systems, and components that can significantly affect safe operation. The design also contains the level of detail necessary to support NRC review and the preparation of procurement specifications and construction and installation specifications. The Combustion Engineering Standard Safety Analysis Report for Design Certification (CESSAR-DC), along with the inspections, tests, analyses and acceptance criteria (ITAAC), has been submitted for NRC review. The NRC's Final Safety Evaluation Report was completed in June 1994 and the Final Design Approval (FDA) was issued in July 1994. Certification of the System 80+ Standard Plant Design by the Commission is expected in 1995. The 10 CFR 52 approach provides a process for resolving licensing issues related to the design before any commitment to construction. A utility can reference a Certified Design and apply for a single combined license, authorizing both construction and operation, with assurance that the NRC staff will not re-review the certified portion of the design. Furthermore, any public hearings undertaken on a specific combined operating license (COL) application would exclude issues related to the certified portion of the standard plant design. This process will allow utilities to plan for new nuclear plants by reducing the uncertainty associated with regulatory delays or design modifications during plant construction and start-up. An overview of the System 80+ design is shown in Figure 1.

Features that contribute to the significant safety improvements of the System 80+ design include:

- Increased reactor core thermal margin achieved by reducing the normal operating hot leg temperature and revising core parameter monitoring methods.
- Use of a ring-forged reactor pressure vessel with improved material specification affording a low 60 year end-of life RTNDT, virtually eliminating pressurized thermal shock concerns. This feature also results in a significantly reduced number of welds (with resulting reduction in in-service inspection).
- Pressurizer volume is increased by 33% (relative to current generation operating reactors), providing more operating margin during plant transients.
- Secondary inventory in the steam generators is increased by 25%, increasing the time period until actuation of reactor protection/safeguards systems and until the steam generator would boil dry without provision of feedwater.

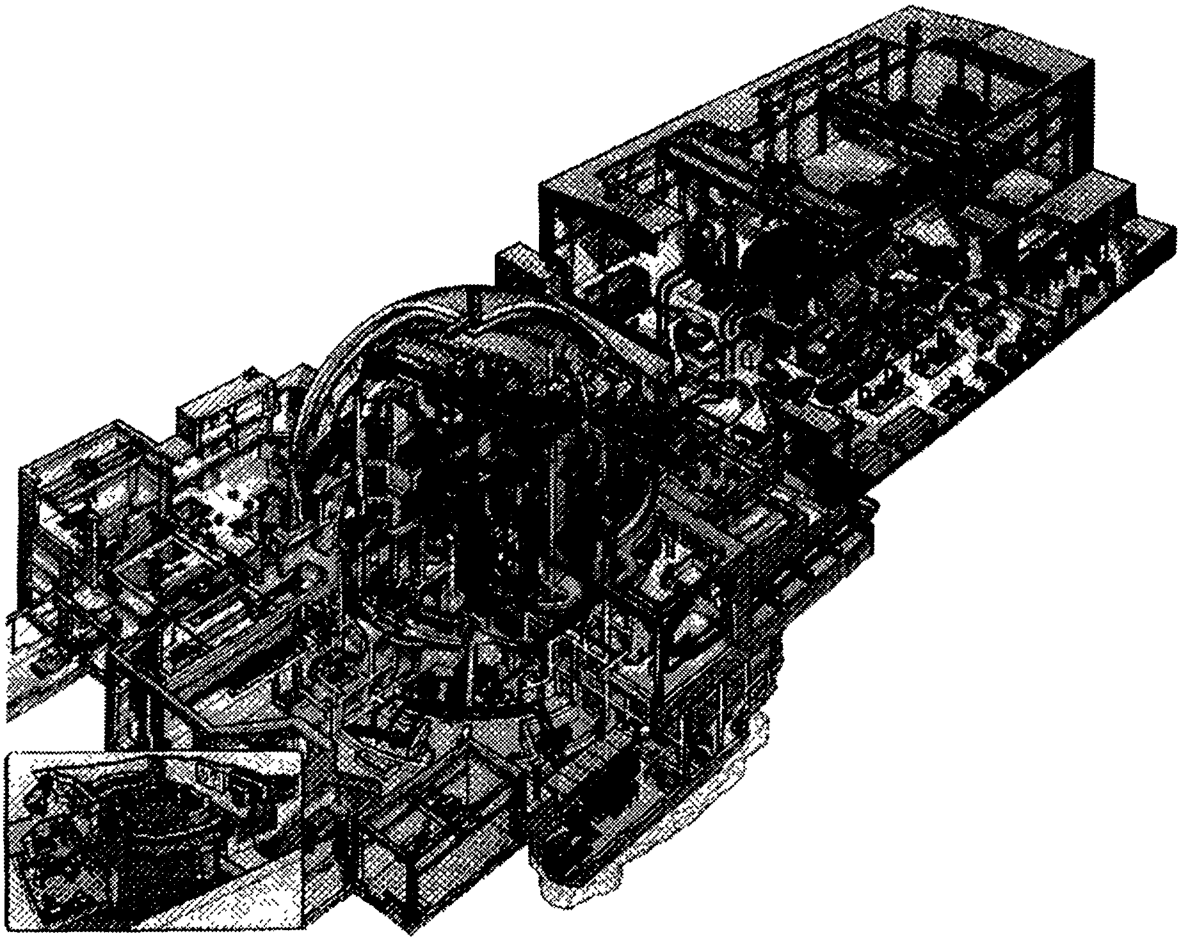


Figure 1: System 80+ Standardized Plant

- Thermally treated Inconel 690 tubing is used to extend the life of the steam generators, improve their reliability and decrease the potential need for plugging tubes over the life of the plant.
- The increases in pressurizer volume and steam generator tubing results in an 8% increase in reactor coolant system inventory above the reactor core providing additional coolant inventory margin for mitigating potential loss of inventory accidents.
- N-16 monitors, one per steam generator, have been incorporated to provide a sensitive and specific indication for primary coolant leakage through steam generators.
- A dedicated Reactor Coolant Pump Seal Injection System has been incorporated. With this system, three levels of protection exist, thereby, essentially eliminating concerns for seal failure and subsequent leakage during periods of prolonged power loss.
- A Safety Depressurization System (SDS) has been added to provide rapid depressurization for severe accident mitigation and for back-up decay heat removal.
- An in-containment refueling water storage tank (IRWST) acts as a quench tank for the SDS, avoids the need for safety injection recirculation switch over to the containment sump after a loss-of-coolant accident, and provides a source of water for cavity flooding.

- A state-of-the-art main control room (Nuplex 80+) using modern human factors engineering techniques and off-the-shelf digital technology has been designed to facilitate the operators' duties during both normal and potential accident situations.
- Hard wired paths for the Plant Protection System (PPS) have been added to provide further diversity to the plants' already redundant Alternate Protection System.
- Additional mechanical redundancy has been provided for the safety injection, emergency feedwater, shutdown cooling, and containment spray systems.
- A large volume containment provides additional margin against overpressuriazation and ensures that global hydrogen concentration cannot reach detonable levels during an accident.
- A hydrogen injector system, in conjunction with hydrogen recombiners, ensures that hydrogen is controlled without global deflagrations.
- A combustion turbine generator provides an alternate source of alternating-current electrical power during loss-of-off site power and station blackout events.

1.2. Plant description

1.2.1. General characteristics

The System 80+ Standard Plant Design represents a complete power plant: nuclear island, turbine island, and balance of plant, which are all integrated for safe, reliable and economic operation.

The Nuclear Steam Supply System (NSSS) is a pressurized water reactor (PWR) with two primary coolant loops, a pressurizer connected to one of the loops, two steam generators, four reactor coolant pumps (RCPs) and the auxiliary and safety systems directly related to the NSSS. The NSSS generates approximately 3931 MWt, producing saturated steam at 1000 psia (6.9 MPa) for use in the balance of plant (BOP) steam and power conversion system. The turbine generator provides a net power of approximately 1350 MWe. Full-load rejection is accepted without reactor or turbine trip. The turbine plant is completely automatic and is supervised from the control room.

1.2.2. Reactor

The reactor vessel is designed to contain and support the core and nuclear fuel. The design is based on the well proven System 80 design. The reactor vessel is a vertically mounted cylindrical vessel with a hemispherical lower head attached to the vessel and a removable hemispherical upper closure head. The reactor vessel is fabricated from low alloy steel and the internal surfaces in contact with reactor coolant are clad with ~nitric stainless steel.

The reactor core consists of 241 fuel assemblies and 93 or more control element assemblies (CEAs). Each fuel assembly is a 16 x 16 array consisting of 236 fuel and poison rods and 5 guide tubes. The fuel rods are Zircaloy tubes containing slightly enriched uranium dioxide pellets. Full-strength CEAs consist of Inconel clad with boron carbide or silver-indium-cadmium absorber rods. Reduced strength control rods composed of solid Inconel provide the capability to change operating power level using control rods only. The

System 80+ approach simplifies reactivity control during plant load changes and reduces liquid waste processing requirements that normally accompany changes in soluble boron concentration.

Reactor vessel internals consist of the core support barrel assembly and the upper guide structure assembly. The core support barrel assembly provides support and location positioning for the fuel assemblies and contains instrument guide paths and hydraulic flow paths. The upper guide structure assembly provides an insertion path and lateral support for the control element assemblies. Reactor vessel internals are designed to withstand the effects of flow induced vibrations caused by operation of the RCPs.

1.2.3. Reactor coolant system

The Reactor Coolant System (RCS) consists of a reactor vessel and two independent parallel loops (Fig. 2). Each loop consists of a 42 inch ID (1065 mm) outlet pipe, two 30 inch ID (760 mm) inlet pipes, a steam generator and two RCPs. The RCPs are electric-motor-driven single-stage centrifugal pumps. The RCS operates at a nominal pressure of 2250 psia (15.5 MPa). System pressure is maintained by an electrically heated pressurizer that is connected to one of the loops. The pressurizer has an increased operating volume relative to previous designs to enhance transient response. Each steam generator is a vertical U-tube heat exchanger used to transfer heat generated in the core. The System 80+ steam generators incorporate several design enhancements including better steam dryers, increased overall heat transfer area and slightly reduced full power steam pressure. The design also provides a larger secondary feedwater inventory which extends the "boil dry" time, thereby enhancing the plant's capability to tolerate upset conditions and improving operational flexibility.

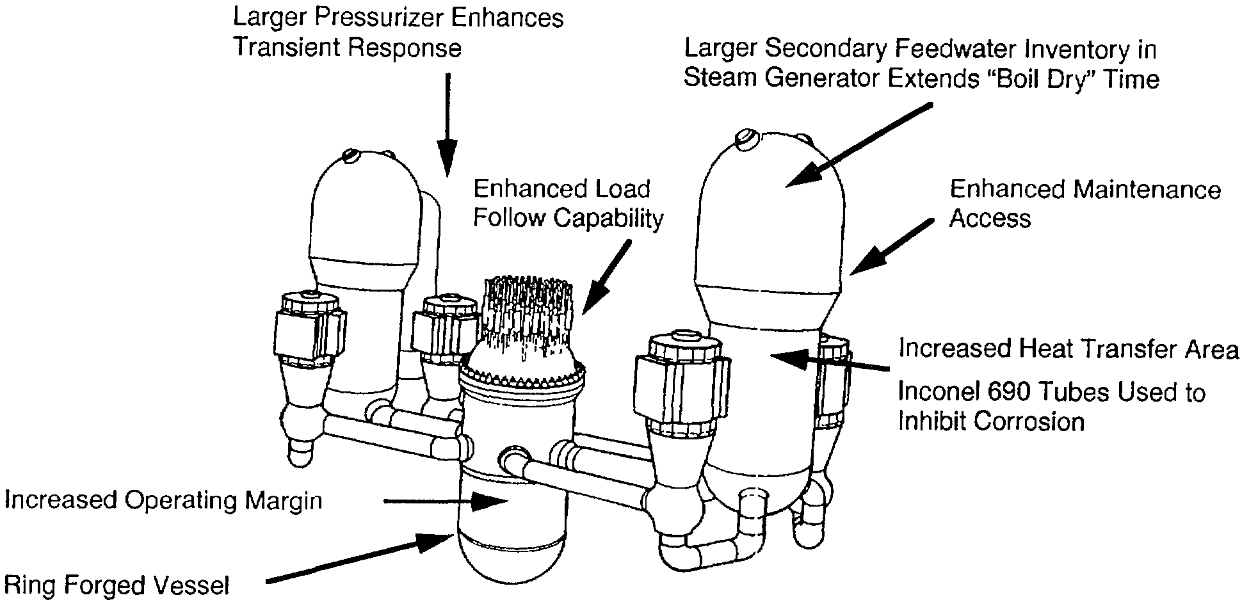

Larger Pressurizer Enhances Transient Response
Larger Secondary Feedwater Inventory in Steam Generator Extends "Boil Dry" Time
Enhanced Load Follow Capability
Enhanced Maintenance Access
Increased Heat Transfer Area
Inconel 690 Tubes Used to Inhibit Corrosion
Increased Operating Margin
Ring Forged Vessel

Figure 2: System 80+ Reactor Coolant System General Arrangement

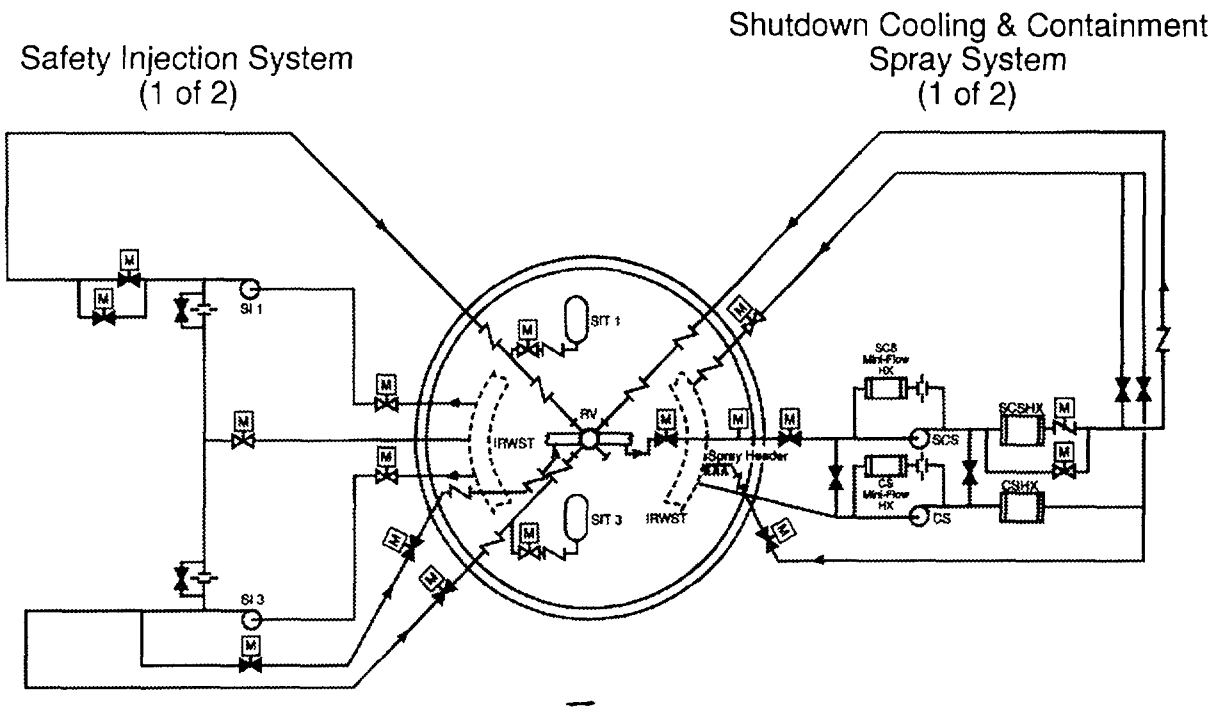
1.2.4. Engineered safety systems

The engineered safety systems consist of the Safety Injection System (S IS), the Safety Depressurization System (SDS), the Emergency Feedwater System (EFWS), the Containment Spray System (CSS), and the Shutdown Cooling System (SCS). These systems are integrated for safe and reliable operation (Fig. 3, 4).

The SIS injects borated water to provide core cooling to limit core damage and fission product release and ensures adequate shutdown margin in the event of a loss-of-coolant accident (LOCA). The SIS is a dedicated four-train system. The SIS pumps take borated water from the in-containment refuelling water storage tank (IRWST) and inject directly into the reactor vessel down comers. Additional borated water injection is provided by pressurized safety injection tanks. The System 80+ approach represents a simpler, more reliable system that eliminates the need to switch from an external water source and provides a semi-closed system with continuous recirculation. The SIS also provides long-term post-accident cooling of the core.

As a backup to the normal pressure control system and the Reactor Coolant Gas Vent System, the SDS provides a safety grade means of depressurizing the RCS. Together with the SIS and SCS, the SDS is capable of providing an alternate means of decay heat removal for those events beyond the plant design basis in which the steam generators are not available. Decay heat removal, via feed and bleed of the RCS, can be accomplished using the SIS to feed the RCS, the SDS to bleed to the IRWST, and the SCS for cooling the IRWST.

The CSS maintains containment pressure and temperature within design limits and scrubs the containment of radioactivity in the unlikely event of design basis mass-energy


Safety Injection System (1 of 2)

Shutdown Cooling & Containment Spray System (1 of 2)

Figure 3: Integrated Engineered Safety Features System

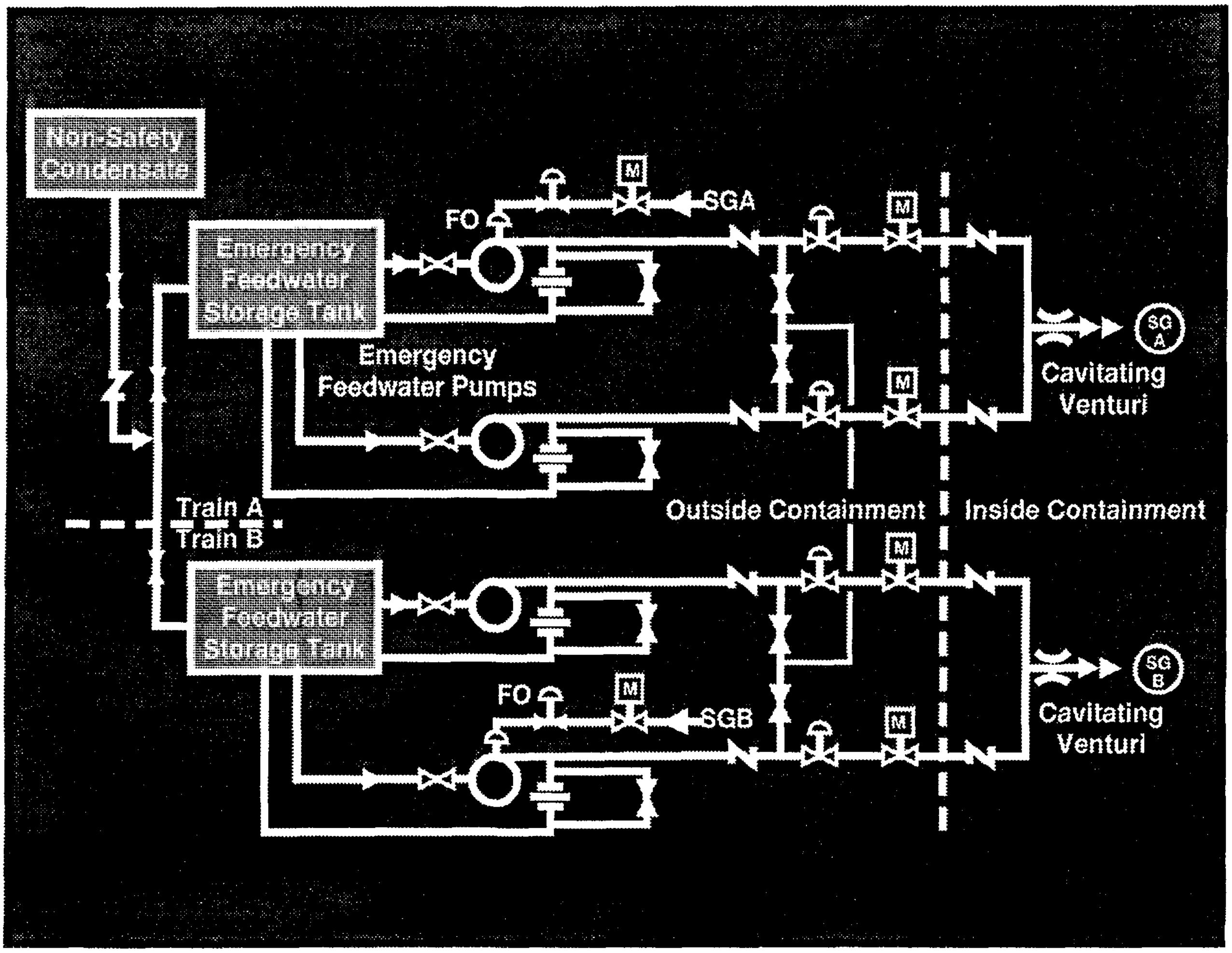


Figure 4: Emergency Feedwater System

release to the containment atmosphere. The CSS pumps take water from the IRWST and thus eliminate the need to switch from an external source. The CSS and SCS are integrated, and their respective pumps are interchangeable; thus backup and higher reliability are provided for both systems.

The EFWS is a dedicated four-train safety system that supplies feedwater to the steam generators for the removal of heat from the RCS in the event the main feedwater system is unavailable following a transient or accident. The EFWS consists of two storage tanks, and four pumps. The design includes cavitating ventures to minimize excess emergency feedwater flow to a steam generator with a broken feed or steam line and thus eliminates the need for automatic isolation of feedwater flow.

The SCS is used to reduce the temperature of the reactor coolant at a controlled rate and to maintain the proper reactor coolant temperature during refuelling. The system has a design pressure of 900 psig (6.3 MPa). This higher system pressure provides for greater operational flexibility and significantly reduces the chance of a large interfacing system LOCA.

1.2.5. Containment

The containment vessel is a 200 ft (61 m) diameter spherical-shaped steel shell with wall thickness of approximately 1 3/4 inch (19 mm). The containment vessel is completely enclosed in a cylindrical reinforced concrete shield building with a hemispherical dome. A 5 ft (1.5 m) annular space between the containment and the shield building is filtered and the air recirculated or exhausted during accident conditions by the annul us ventilation system. Space below the containment and inside the shield building houses the engineered safety systems (Fig. 5).

Use of spherical steel containment provides 75% more space on the operating floor than does a typical cylindrical containment of equal volume. Allowance is made for one piece steam generator removal. Quadrant division and physical separation of safety components virtually eliminate concerns of fire, flood, and sabotage (Fig. 6). A cylindrical, concrete shield building provides the additional protection from external hazards (e.g., severe weather, aircraft impact, etc.) as well as providing radiation shielding.

1.2.6. Plant protection system

The Plant Protection System (PPS) consists of the Reactor Protective System (RPS) and the Engineered Safety Features Actuation System (ESFAS). The RPS automatically initiates a reactor trip when any of the monitored process variables reach a trip set point. The ESFAS provides an actuation signal to the engineered safety features systems when any of the monitored process variables reach a predetermined set point. The PPS is augmented by the Alternate Protection System which generates an alternate reactor trip signal and an alternate emergency feed water actuation signal that is independent and diverse from the PPS. The PPS employs automatic on-line functional testing to eliminate most periodic surveillance tests.

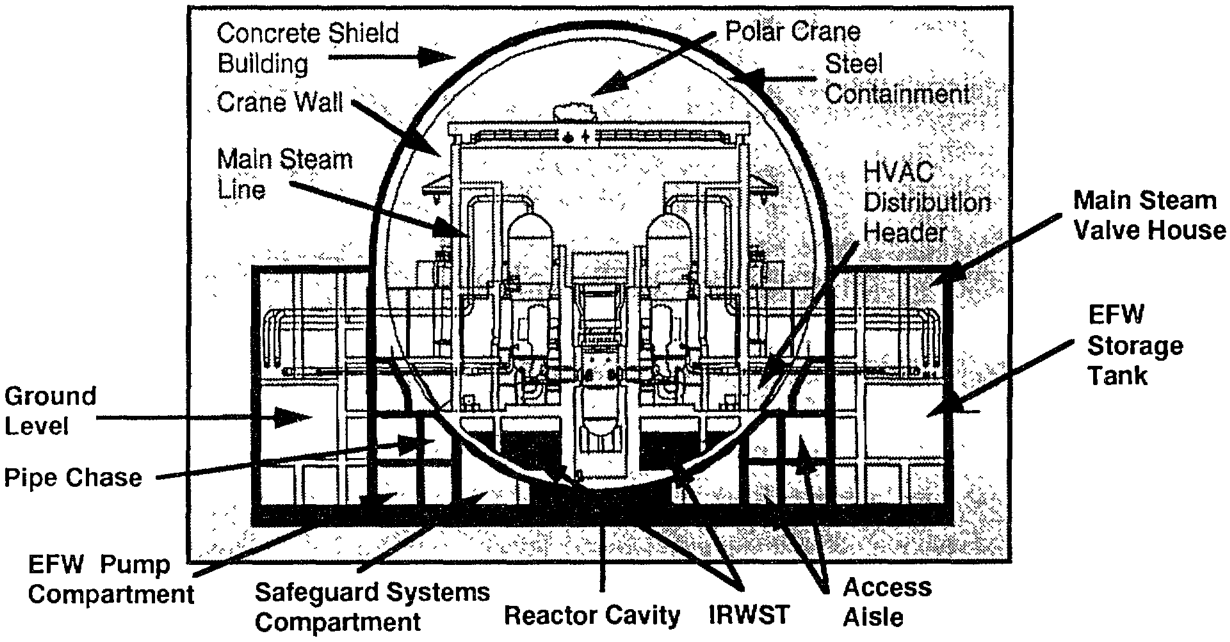


Figure 5: System 80+ Spherical Steel Containment

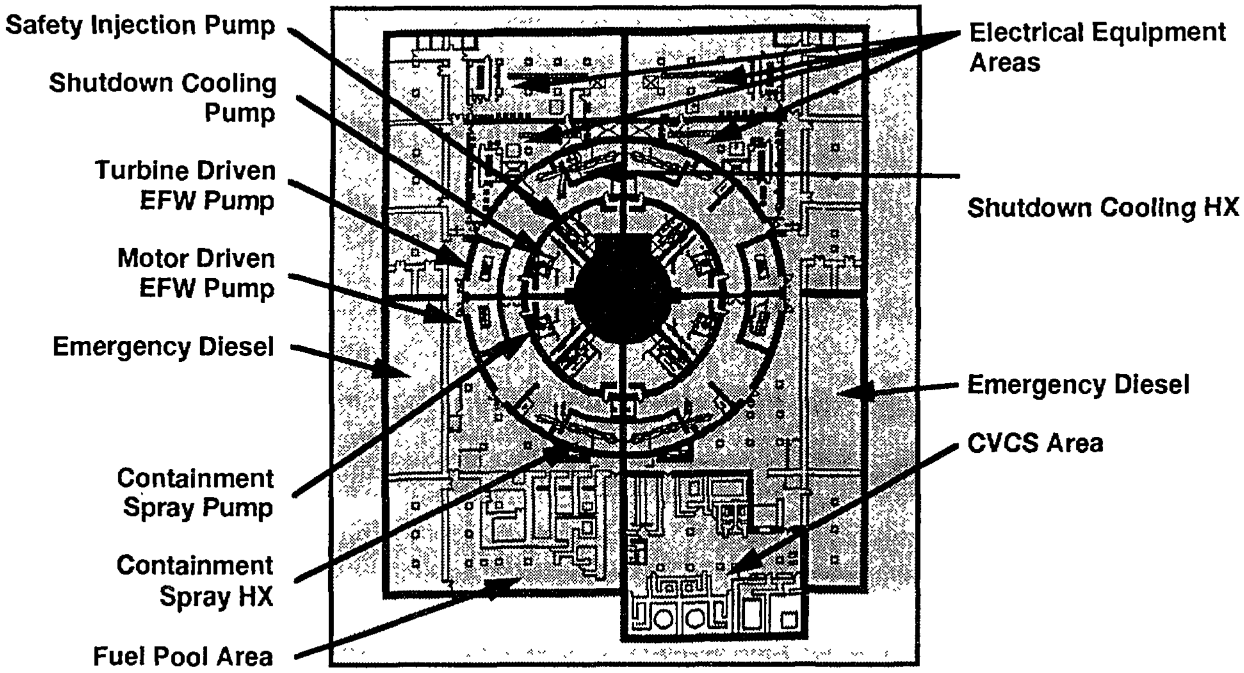


Figure 6: General Arrangement of Containment and Nuclear Annex (Basemat Level)

The trip set points of the RPS are selected to ensure that design basis events do not cause the violation of specified acceptable fuel design limits (SAFDLs). The reactor trip also helps ensure that the engineered safety systems are actuated to minimize the effects of anticipated operational occurrences (AOOs).

1.2.7 Steam and power conversion system

The Steam and Power Conversion System converts the heat energy generated in the reactor into electrical energy. The system utilizes the Main Steam System, the high pressure and low pressure turbines, the main generator and a condensing cycle with regenerative feed water heating. A turbine bypass system and atmospheric dump valves are available to dissipate heat from the reactor during a turbine and/or reactor trip. The turbine-generator produces a net electric power of 1350 MWe.

1.2.8. Nuplex 80+ advanced control complex

The Nuplex 80+ Advanced Control Complex (ACC) is a plant wide computer based control and monitoring systems design (Fig. 7). The complex consists of Main Control Panels (MCPs), Remote Shutdown Panel (RSP), Discrete Indicating and Alarm System (DIAS), Data Processing System (DPS), and Component Control System (CCS). The ACC makes extensive use of remote multiplexing, digital computers, color graphic displays and fiber-optic data communications. The control complex design integrates monitoring and control of both nuclear and balance-of-plant systems.

The master control console, consisting of five MCPs, are designed for one person seated operation of the plant from hot standby through full power modes of operations. How-

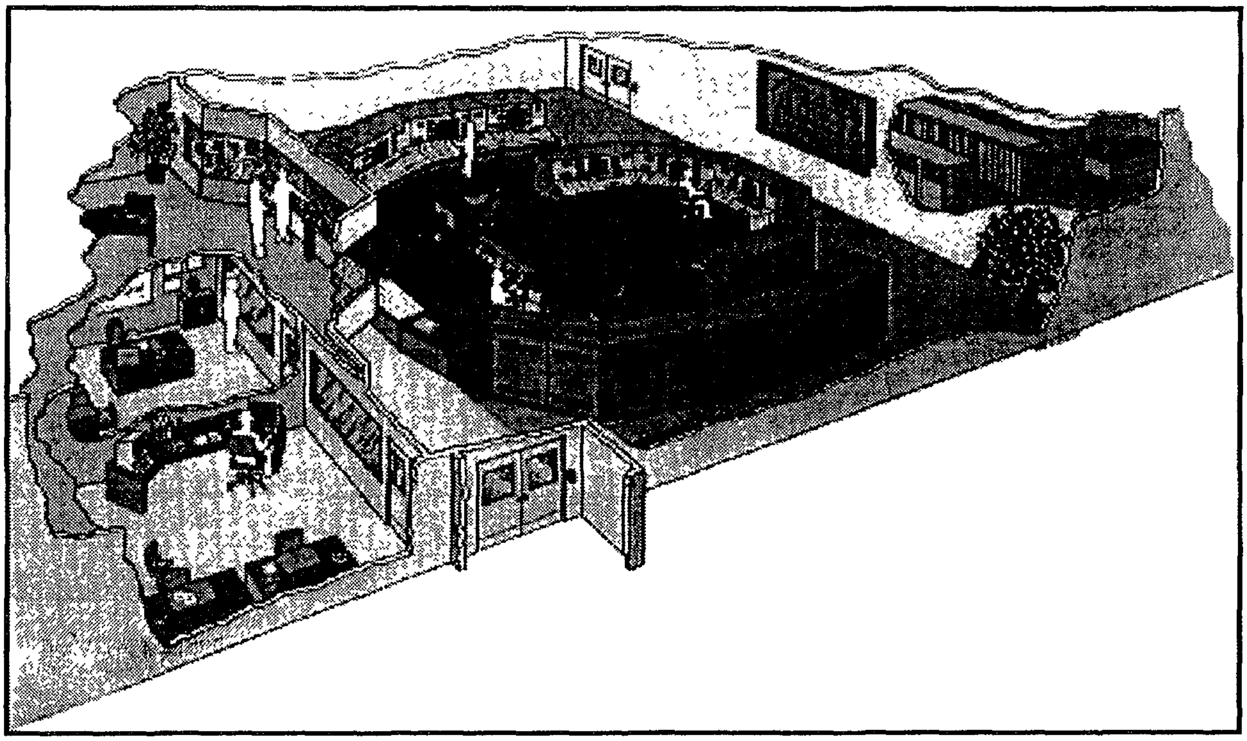


Figure 7: Nuplex 80+ Advanced Control Complex

ever, the main control room design accommodates two control room operators and a supervisor for all normal modes of plant operation and additional operating staff during emergencies.

The arrangement and layout of the MCPs were established based on the coordinated design effort of a team of human factors specialists, reactor operators, instrumentation and control engineers, architectural engineers and owner utility designers. Each MCP employs alarm modules, a color graphic CRT, discrete indicators, process controllers and control switches as the primary man-machine interfaces.

The RSP design includes a minimum of two isolated redundant channels of the safety-related instrumentation and controls necessary to achieve hot standby if the main control room must be evacuated. Additionally, local controls, RSP controls, and instrumentation are provided to bring the plant to cold shutdown conditions using applicable procedures.

The DIAS is a fixed position indication and alarm system that utilizes flat panel display devices. The DIAS is designed to aid the operator in handling any challenges to critical plant safety functions. The DIAS allows continuous monitoring of safety functions including reactivity control, RCS inventory control, RCS pressure control, core heat removal, RCS heat removal, containment integrity, and plant radiation emission.

The DPS is a fault tolerant multiprocessor computer based system which provides plant data and status information to the operations staff. The plant operations staff obtain detailed process data via CRT information output devices. The major functions performed by the DPS include plant wide data acquisition via dedicated data links to other plant systems, validation of sensed parameters, execution of application programs and performance calculations, monitoring of general plant status and plant safety status, generation of logs and reports, the determination of alarm conditions, sequence of events recording and post-trip review. Multicolor CRTs with touch-screen control and high speed printers are used to present the plant information to the operators.

The CCS is designed to control discrete-state components such as pumps, valves, heaters and fans within plant systems. The CCS consists of the ESF-CCS and Process CCS assemblies to provide control for the different channels of Class lE equipment, as well as non-Class lE equipment.

An Integrated Plant Status Overview (IPSO) panel is a large screen display device that is included in the Nuplex 80+ ACC to provide the operators and supervisory staff with a quick means of assessing the plant status from anywhere in the controlling work space.

The ACC also includes adjacent offices and an overlooking Technical Support Center (TSC) for the operation staff. Each office includes a viewing window into the control room, and a CRT that provides access to the same display pages as are provided by the control room CRTs.

1.3. Design basis accidents

The System 80+ Standard Plant Design has been analyzed to ensure that it can withstand anticipated operational occurrences as well as a broad spectrum of postulated accidents without posing undue risk to the public health and safety. The following categories of initiating events have been analyzed:

1.3.1. Increase in heat removal by the secondary system

- decrease in feedwater temperature
- increase in feedwater flow
- increase in steam flow
- inadvertent opening of a steam generator relief or safety valve

1.3.2. Decrease in heat removal by the secondary system

- loss of external load
- turbine trip
- loss of condenser vacuum
- main steam isolation valve closure
- loss of non-emergency ac power to the station auxiliaries
- loss of normal feedwater flow
- feedwater system pipe breaks

1.3.3. Decrease in reactor coolant flow rate

- total loss of reactor coolant flow
- single RCP rotor seizure with loss of off site power (LOOP)
- RCP shaft break with LOOP

1.3.4. Reactivity and power distribution anomalies

- uncontrolled CEA withdrawal from a subcritical or low power conditions with LOOP

- uncontrolled CEA withdrawal at power
- single CEA drop
- startup of an inactive RCP with & without single failure
- inadvertent deboration
- inadvertent loading of a fuel assembly into the improper position
- CEA ejection

1.3.5. Increase in reactor coolant system inventory

- inadvertent operation of the SIS
- chemical and volume control system malfunction (pressurizer level control system malfunction with LOOP)

1.3.6. Decrease in reactor coolant system inventory

- double-ended break of a letdown line outside of containment
- steam generator tube rupture with and without LOOP and with LOOP stuck open ADV
- loss-of-coolant accident (LOCA)

1.3.7. Radioactive material release from a subsystem or component

- postulated radioactive release due to liquid-containing tank failure
- fuel handling accident
- spent fuel cask drop accident

1.3.8. Containment depressurization faults

- inadvertent operation of fan cooler system
- inadvertent operation of containment purge system
- inadvertent operation of containment sprays

1.4 Severe Accidents

The System 80+ Standard Plant Design provides a more resilient plant designed to minimize the potential for core damage and to moderate the severity of a severe accident in the unlikely event one should occur. Design features that contribute to the significant improvement for the above stated functions include a robust containment design, Reactor Cavity Flood System, Hydrogen Mitigation System, Safety Depressurization System, and integrated Shutdown Cooling and Containment Spray Systems. The PRA performed for the System 80+ Standard Plant Design indicates a significant improvement in the total core damage frequency as a result of incorporating the above features. The total core damage frequency for the System 80+ Standard Plant Design (with the reactor initially at full power) is 2.8 x 10^{-6} events/yr. This represents more than two orders of magnitude improvement over its predecessor and surpasses the EPRI ALWR URD goal of 1.0 x 10^{-5} events/yr.

With the reactor initially shutdown, it has been shown that the risk of core damage has been reduced by a factor of 40.

New radiological source term technology developed by the U.S. Nuclear Regulatory Commission was used along with a more detailed model for containment spray cleanup effectiveness. This resulted in a site boundary dose for a large LOCA-initiated severe accident that is significantly less than the Protective Action Guideline for initiation of emergency evacuation.

2. DESCRIPTION OF KEY FEATURES IN 15 DESIGN AREAS AS SELECTED FROM INSAG-3

In the following sections the reference to INSAG-3 is put in parentheses after each heading.

2.1. Plant process control systems (4.2.2.1)

The Power Control System and the Process-Component Control System (PCS/PCCS) are non-safety related instrument and control systems which provide control functions to maintain the plant within its normal operating range for all normal modes of plant operation. The PCS/P-CCS provide the following control functions:

- reactivity control using control element assemblies,
- pressurizer pressure and level,
- power change limiter,
- main feed water flow,
- reactor power cutback,
- main steam bypass flow,
- boron concentration,
- alternate reactor trip actuation, and
- alternate emergency feedwater actuation.

2.2. Automatic safety systems (4.2.2.2)

The Plant Protection System (PPS) is a safety-related instrumentation and control system which initiates a reactor trip and actuation of engineered safety features in response to plant conditions monitored by process instrumentation. The PPS consists of the Reactor Protective System (RPS) and the Engineered Safety Features Actuation System (ESFAS). The RPS initiates a reactor trip if the reactor conditions approach prescribed safety limits. The ESFAS actuates the engineered safety features systems.

2.2.1. List of automatic safety systems

- Reactor Protective System (RPS)
- Containment Isolation System (CIS)
- Mainsteam Isolation System (MSIS)
- Safety Injection System (SIS)
- Emergency Feedwater System (EFWS)
- Containment Spray System (CSS)

2.2.2. Reactor protective system

The RPS rapidly shuts down the reactor when certain plant conditions approach safety system set points. The RPS is segregated into four completely independent channels consisting of sensors, transmitters, signal conditioning equipment, and digital equipment which performs the calculations and logic to generate protective function initiation signals.

2.2.3. Containment isolation system

The CIS provides a means of isolating fluid systems that pass through containment penetrations so that any radioactivity that may be released into the containment following a design-basis accident will be confined within the steel containment building. The CIS provides a pressure barrier at each containment penetration. Valves that must be isolated are installed with air-operated controllers or motor-operated controllers. Lines that must remain in service following an accident have at least one remote manual valve.

2.2.4. Main steam isolation system

The MSIS isolates the steam line piping and the main feed water piping associated with a steam generator following a steam generator tube rupture, a main steam line break, or a main feed water system upset. An MSIS isolation signal is initiated upon receipt of a high containment pressure signal, a low steam generator pressure signal, or a high steam generator water level signal.

2.2.5. Safety injection system

The SIS injects borated water directly into the reactor vessel to provide core cooling and reactivity control in response to design basis accidents. The system also provides core cooling during feed and bleed operation in conjunction with the Safety Depressurization System (SDS). Operation of the system is initiated in the event of low RCS pressure or high containment pressure.

The SIS consists of two divisions. Each division has two safety injection pumps, two safety injection tanks, valves, piping, and instrumentation and controls. The system uses the IRWST for its source of injection water for the high pressure safety injection pumps. Two safety injection pumps in conjunction with the safety injection tanks have the capacity to cool the core during design basis events.

The system is capable of injecting highly borated water into the RCS to mitigate LOCAs, a steam generator tube rupture, a steam line break, or a CEA ejection. Additionally, the system is capable of providing an alternate means of decay heat removal for those events that are beyond the plant design basis in which the steam generators are not available.

2.2.6. Emergency feedwater system

The EFWS provides emergency feedwater to the steam generators to ensure the capability to remove decay heat from the RCS for events resulting in loss of normal feedwater and requiring the removal of heat from the RCS through the steam generators. This includes the loss of normal on site and normal off site AC power.

The EFWS consists of two divisions, each with a storage tank, two EFW pumps, a cavitating flow-limiting venture, valves, piping, instrument and controls. The EFW pumps in each division are powered by diverse drives (i.e., motor-driven and turbinedriven). The cavitating flow-limiting ventures limit emergency feedwater flow to each steam generator with both EFW pumps running in the division against steam generator pressures down to 0 psig.

2.2.7. Containment spray system

The CSS reduces containment pressure and temperature and reduces the concentration of radio-nuclides (released from fuel) from the containment atmosphere following a main steam line break (MSLB) inside the containment or a LOCA inside the containment.

The CSS consists of two divisions. Each division has a containment spray pump, a heat exchanger, a spray header, valves, piping, controls and instrumentations. The system uses the IRWST for its source of spray water.

Each CSS division has the heat removal capacity to cool and depressurize the containment atmosphere such that containment design pressure and temperature are not exceeded following a LOCA or MSLB.

2.3. Protection against power transient accidents (4.2.3.1)

Two independent reactivity control systems of different design principle are provided. The first system, using CEAs, includes a positive means (gravity) for inserting CEAs and is capable of reliably controlling reactivity changes to assure that under conditions of normal operation, including anticipated operational occurrences, SAFDLs are not exceeded. The CEAs can be mechanically driven into the core. The second system, using neutron absorbing soluble boron, is capable of reliably compensating for the rate of reactivity changes resulting from planned normal power changes such that SAFDLs are not exceeded. This system is capable of holding the reactor subcritical under cold conditions.

Either system is capable of bringing the core to a subcritical condition from a hot operating condition and holding it subcritical in the hot standby condition. The CEAs are designed so that the potential amount and rate of reactivity insertion from the reactivity control systems under normal operation and postulated reactivity accidents do not result in violation of the SAFDLs, damage to the reactor coolant pressure boundary (RCPB) or disruption of the reactor core or internals which would impair the ability to provide safety injection of reactor coolant.

2.4. Reactor core integrity (4.2.3.2)

The reactor core is designed with appropriate margin to assure that SAFDLs are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences. The System 80+ design criteria includes:

- The minimum departure from nucleate boiling ratio (DNBR) during normal operation and anticipated operational occurrences will provide at least a 95% probability with 95% confidence that departure from nucleate boiling does not occur.
- The maximum fuel centerline temperature evaluated at the design temperature overpower condition is below that value which could lead to centerline fuel melting. The melting point of UO_2 is not reached during normal operation and anticipated operational occurrences.
- Fuel rod clad is designed to maintain cladding integrity throughout fuel life.
- The reactor system is designed so that any xenon transients will be adequately damped.

- The reactor is designed such that the combined response of the fuel temperature coefficient, the moderator temperature coefficient, the moderator void coefficient, and the moderator pressure coefficient to an increase in reactor thermal power is a decrease in reactivity. The reactor is designed such that the moderator temperature coefficient is negative at all power levels throughout the entire operating cycle. In addition, reactor power transients remain bounded and damped in response to any expected changes in any operating variable.
- The RCS is designed and constructed to maintain its integrity throughout the expected plant life. The reactor and PPS are designed such that power excursions that could result from any credible reactivity addition incident do not cause damage either by deformation or rupture of the pressure vessel, or impair operation of the engineered safety features.

2.5. Automatic shutdown systems (4.2.3.3)

The RPS is designed to rapidly shutdown the reactor when certain plant conditions approach safety system set points. Set points for initiation of a reactor trip are installed for each monitored condition to provide for initiation of a reactor trip prior to exceeding reactor coolant pressure boundary limits or fuel thermal limits for anticipated operational occurrences. The system is segregated into four completely independent channels. The system consists of a sensor/transmitter, signal conditioning, stable logic, digital equipment which performs the calculations and logic to generate protective function initiation signals, local coincidence logic, and initiating relays.

The system monitors the following plant conditions to provide a reactor trip when necessary:

- reactor power - high
- linear heat generation rate - high
- departure from nucleate boiling ratio - low
- reactor coolant system pressure - high or low
- steam generator water level - high or low
- steam generator pressure - low
- containment pressure - high
- reactor coolant flow - low

2.6. Normal heat removal (4.2.3.4)

The RCS circulates water in a closed cycle, removing heat from the reactor core and internals and transferring it to a secondary system. The steam generator provides the interface between the RCS and the Main Steam System (MSS). The MSS transports steam from the steam generators to the power conversion system. The turbine generator is a non-safety system that converts the energy of the turbine steam produced in the steam generators into mechanical shaft power and then into electrical energy.

The SCS can cool the RCS from the SCS entry condition to 200°F (93°C) within 24 hours after reactor shutdown with only one SCS heat exchanger in operation.

2.7. Emergency heat removal (4.2.3.5)

The design objective for the System 80+ engineered safety systems is to provide protection in the highly unlikely event of an accidental release of radioactive fission products from the RCS particularly as the result of a LOCA. The systems function to localize, control, mitigate, and terminate such incidents and to hold exposure levels below the limits in 10 CFR 100. This is accomplished by highly reliable and redundant engineered safety systems: the SIS, the EFWS, the SCS, and the SDS.

The SIS injects borated water into the reactor vessel to provide reliable core cooling and additional reactivity control capability. Additionally, the SIS provides core cooling during feed and bleed operation in conjunction with the SDS. The four train safety injection pumps, the four safety injection tanks, and the IRWST are utilized to provide core cooling for the complete spectrum of reactor coolant pipe breaks.

The EFWS provides an independent safety related means of supplying secondary side feedwater to the steam generators for removal of heat and prevention of reactor core uncovery.

The SCS removes heat from the reactor coolant and transfers the heat to the Component Cooling Water System during reduced RCS pressure and temperature conditions. The system provides low temperature over pressure protection for the RCS. Pressure retaining components have a design pressure of at least 900 psig (6.3 MPa) and a design temperature of at least 400°F (204°C).

The SDS is composed of two subsystems. The Reactor Coolant Gas Vent System (RCGVS) provides a means to vent steam and non-condensible gases from the pressurizer and the reactor vessel upper head (RVUH). The Rapid Depressurization System (RDS) provides a rapid depressurization of the RCS by venting the pressurizer. The SDS consists of two redundant RDS piping trains from the pressurizer to the IRWST, and two RCGVS piping trains, one from the pressurizer and one from the RVUH, which discharge to either the reactor drain tank (RDT) or the IRWST. The RCGVS depressurizes the RCS at a rate of at least 0.9 psi per second (6kPa/s) at an initial pressurizer pressure of 2250 psig (15.6 MPa).

The RCGVS venting capacity is adequate to depressurize the RCS following design basis events. The RDS depressurization capacity, in conjunction with SIS operation, will prevent uncovering the core during a total loss of feedwater (TLOFW). A single RDS train in conjunction with two of four safety injection pumps prevent core uncovery following a TLOFW if feed and bleed is initiated immediately following the opening of pressurizer safety valves (PSVs). The two RDS trains have sufficient total flow capacity with all safety injection pumps operating to prevent core uncovery following a TLOFW if feed and bleed is delayed up to 30 minutes from the time PSVs lift.

2.8. Reactor coolant system integrity (4.2.3.6)

2.8.1. General

RCS components are designed, constructed and operated in accordance with the applicable ASME codes. The RCPB is designed to accommodate the system pressures and temperatures attained under all expected modes of unit operation including all anticipated transients, and maintain the stresses within applicable limits. Piping and equipment pressure parts of the RCPB are assembled and erected by welding unless applicable codes permit flanged or screwed joints. All welding procedures, welders and welding machine operators qualifies in accordance with applicable ASME codes. The RCPB includes all pressure vessels, piping, pumps and valves which are part of the RCS and others connected to the RCS.

Required pre-service and in-service inspections are performed on the system. Additionally, the NSSS integrity monitoring system which consists of the Internals Vibration Monitoring System, the Acoustic Leak Monitoring System and the Loose Parts Monitoring System can help to detect defects or deformation in the RCS.

2.8.2. Primary system overpressure protection

Overpressure protection of the RCPB is provided by the pressurizer safety valves (PSVs), main steam safety valves (MSSVs), and relief valves of the SCS.

Four spring-loaded PSVs are located on piping connected to the top of the pressurizer. The PSVs discharge to the IRWST. PSV set pressure equals 2500 psia ± 25 psi (17.2 MPa ± 1%) and the minimum capacity of each valve is 535,000 lb/hour (243 t/h).

The MSSVs provide over pressure protection for the secondary side of the steam generators and for pressure boundary components in the MSS. The MSSVs are direct acting, spring loaded, carbon steel valves. The valves are mounted on each of the main steam lines upstream of the steam line isolation valves, and outside containment.

Over pressure protection of the RCS during low temperature conditions is provided by the relief valves located in the SCS.

2.8.3. Inspection and test of the primary pressure boundaries

The purpose of the in-service inspection program is to periodically monitor the system or components in order to identify and to repair those indications which do not meet acceptance standards. The program includes:

- hydrostatic test program;
- pump and valve in-service program which requires operability testing of selected pumps and valves;
- component inspection program which includes piping system welds, hangers, supports, internal inspection of pump and valve bodies;
- pre-service inspection program.

2.8.4. Determination of leaks through the steam generator

An increase in radioactivity indicated by main condenser evacuation system monitor, and blow down system monitors will reveal primary reactor coolant leakage through steam generators tubes to the secondary side. Routine analysis of steam generator secondary water samples will also indicate increasing leakage of reactor coolant into the secondary system. Additionally, the System 80+ Standard Plant Design incorporates two N-16 monitors, one per steam generator, to provide a sensitive and specific indication for primary coolant leakage through steam generator tubes.

The System 80+ steam generators have the following design features which enhance the corrosion resistance properties:

- steam generator tubes made of thermally treated inconel 690;
- steam, feedwater and condensate systems employing materials resistant to corrosion and the generation of corrosion products which can be transported into the steam generators;
- high capacity steam generator blow down system; and
- secondary circulation system for chemistry control during wet lay up.

2.8.5. Reactor vessel integrity

The System 80+ reactor vessel is designed to contain and support the core and fuel. A major improvement in manufacturing and operation has been achieved through the use of ring forging. The use of ring forging as opposed to rolled and welded plates used in previous vessel designs reduces the number of welds and the overall complexity of the vessel. Furthermore, the remaining welds have been relocated to areas of lower neutron flux thus enhancing the vessel's resistance to brittle fracture.

The reactor vessel is fabricated from low alloy steel with controlled copper, nickel, sulfur, and phosphorous content in the belt line region of the vessel.

The reactor vessel is designed and constructed in accordance with the ASME code. Test and inspection requirements of the reactor vessel exceed the ASME code requirements. Test and inspection requirements assure that flaw sizes are limited so that the probability of failure by rapid propagation is extremely remote.

Excessive embrittlement of the reactor vessel material due to neutron radiation is prevented by providing an annul us of coolant water between reactor core and the vessel. In addition, to minimize the effects of irradiation on material toughness properties of core belt line materials, restrictions on upper limits for residual elements that directly influence the RTNDT shift are required by the design specification. Specifically, upper limits are placed on copper, nickel, phosphorous, sulfur, and vanadium.

The maximum integrated fast neutron flux exposure of the reactor vessel wall opposite the mid plane of the core is less than 6.2E19 nvt. This value assumes a sixtyyear vessel design life and an eighty percent plant capacity factor. The maximum expected increase in transition temperature is about 79°F (44°C). The actual change in material toughness properties due to irradiation will be verified periodically during plant lifetime by a material surveillance program. Based on an initial RTNDT of 10°F (-12°C), no operating restrictions are necessary to limit vessel stresses.

2.8.6. Materials of the primary pressure boundaries

The materials used for construction of components of the RCPB are in accordance with the ASME code. The materials of construction of the RCPB exposed to the reactor coolant are selected to minimize corrosion and have previously demonstrated satisfactory performance in other existing operating reactor plants. Additionally, the test and inspection requirements of all the RCPB components are in accordance with the ASME code. The test and inspection requirements assure that flaw sizes are limited so that the probability of failure by rapid propagation is extremely remote.

2.9. Confinement of radioactive material (4.2.3.7)

For normal RCS conditions and operational occurrences, the fuel system and the provide barriers against the release of radioactive material generated by nuclear reaction. For design basis accidents, the containment minimizes or prevents the release of radioactive materials as the containment retains its integrity at the temperature and pressure associated with the most limiting design basis accident. For severe accidents, the Reactor Cavity Flood System provides coolability and retention of molten core debris, and hydrogen igniters accommodate 100% of the core metal-water reaction and maintain hydrogen concentration below 10% by volume to ensure containment integrity.

2.10. Protection of confinement structure (4.2.3.8)

2.10.1. Loads acting upon the outer protective shell of the containment

Seismic effects

The System 80+ design is not based on a specific site. It envelopes the design basis earthquakes at the majority of potential plant sites in the continental U.S. Normal operating and accident loads are appropriately combined with the seismic loads and allowable stress limits and deformations are defined so that critical safety functions are not jeopardized. The safe shutdown earthquake (SSE) peak ground acceleration of 0.3 g is selected.

Loads due to wind, hurricane and tornado

The concrete shield building is designed to withstand, without loss of function, the effects of any one of the most severe natural phenomena. A design wind velocity of 110 mph (49 m/s) and a maximum tornado wind velocity of 330 mph (147 m/s) is used.

External industrial hazards and airplane crash

Frequent external hazards are treated deterministically based on criteria given in USNRC Regulatory Guides (Administrative control of transportation and storage of hazardous materials on-site, toxic gas and smoke monitors closing control room ventilation intake, site selected outside the radius of influence of potential off site hazardous materials.) Infrequent external hazards are evaluated in the PRA. Aircraft hazards frequency is minimized by siting criteria. Using the siting criteria (plant to airport distance, plant to edge of military training route, plant to edge of federal airway holding pattern or airport), the probability of an aircraft impact at the site which leads to core damage is less than 10^{-8} events per year. Additionally, the System 80+ design features a dual protection approach. The inner, leak-tight sphere of one and three-quarter inches thick welded steel is surrounded by the three foot thick reinforced concrete shield building. This secondary containment protects the internal steel containment from external hazards. Redundancy in the electrical distribution system with physical separation protects against a single transportation accident causing a

LOOP. The Ultimate Heat Sink has redundancy to ensure a single transportation accident can not cause loss of heat sink.

2.10.2. Protection against external pressure loading

A vacuum load can be imposed on the containment vessel by an inadvertent actuation of the CSS during normal unit operation. The design vacuum pressure is -2.0 psig (-13.8 kPa).

2.10.3. Containment protection against internal pressure

The design basis loads are based on the peak pressure and temperature developed inside the containment as a result of a rupture in the primary coolant system up to and including a double-ended rupture of the largest pipe or a main steam line break. The containment design pressure is 53 psig (0.365 MPa) and the design temperature is 290°F (143°C).

The containment systems include the Steel Containment Vessel, the Containment Spray System, the Containment Air Purification and Cleanup Systems, the Containment Isolation System and the Containment Combustible Gas Control System.

The safety design basis for the containment is the requirement that the release of radioactive materials subsequent to an accident does not result in doses in excess of the values specified in 10 CFR 100. The containment must withstand the pressure and temperature of the design basis accidents without exceeding the design leakage rate of 0.5% volume for the first 24 hours and the volume thereafter is based on a leak rate associated with half of the peak pressure assuming 0.5% volume leak rate at peak pressure.

No special provisions for protection against loss of containment integrity under external loading conditions are required. Considerations given to inadvertent operation of containment heat removal systems and other possible modes of plant operation that could potentially result in significant external structural loading has resulted in pressure lower that the design containment external pressure. The minimum calculated pressure is -1.83 psig (-12.6 kPa). A nominal pressure of -2.0 psig (-13.8 kPa) has been used for the design.

2.11. Monitoring of plant safety status (4.2.3.9)

The ACC uses an integrated information hierarchy to present both safety-related and non-safety-related plant data for use by the control room operators. An integrated system ensures that the operator will be familiar with information displays during abnormal transients since the operator uses the same displays for both normal and abnormal operations. These distinct information display systems are regularly used by the operator: the IPSO panel, the DPS, and the DIAS. These display systems have been designed and configured such that the loss of any one of them does not result in a loss of necessary information to monitor plant safety.

The IPSO panel receives data from both the DIAS and DPS via different data links. The IPSO keeps operations personnel informed about the status of the plant's critical safety functions and success paths. It also provides a limited set of key plant parameters.

The DPS is configured redundantly for improved reliability. It acquires plant data (e.g., process variable and component status), validates it, and executes applications programs for its display hierarchy. The IPSO, critical safety functions, and success path monitoring are the portion that aid the operator in gathering supporting information and problem diagnosis.

The DIAS employs discrete indicators that are used to display validated safety and non-safety-related plant process parameters. It uses a segmented design to provide a degree of hardware independence and fault resistance between various segments. The DIAS channel P segment is designed to be physically separate from and electrically independent of the remaining DIAS channel N segment and the DPS such that a single failure will not cause a loss of more than one of the three display methods.

2.12. Preservation of control capability (4.2.3.10)

The RSP provides an alternate control station which can be used to shutdown the plant in the unlikely event that the main control room becomes uninhabitable. Sufficient safety grade instrumentation and controls are provided to perform the following operations:

- Achieve prompt hot shutdown of the reactor.
- Maintain the plant in a safe condition during hot shutdown.
- Achieve and maintain cold shutdown of the reactor from the RSP.

The RSP design is based on the standard Nuplex 80+ indication and control methodologies. It applies the human factor design criteria in a manner consistent with the MCP design. Also, the indication and control at the Nuplex 80+ RSP are physically separated and electrically isolated from the Nuplex 80+ main control room.

2.13. Station blackout (4.2.3.11)

The System 80+ Standard Plant Design provides the following design features to ensure a safe shutdown of the reactor in the event of a station blackout:

- one turbine-driven emergency feedwater pump is included for each steam generator (this is in addition to the two motor-driven emergency feedwater pumps).
- each of the four safety-related instrument channels has a battery backup. In addition, Class IE Electrical Division I and II, which include the diesel generators, have their own batteries.
- the design has full load rejection capability and the capability to subsequently provide electrical power for house loads from the turbine generator.
- an alternate source of AC power which is diverse from the safety-grade emergency diesels is included. This alternate AC is a control-grade gas turbine and has its own battery.

2.14. Control of accidents within the design basis (4.2.3.12)

A systematic approach to plant operations based on a hierarchy of protective actions is utilized. The protective actions, are directed at mitigating the consequences of an event and once fulfilled, ensure proper control of the event in progress. A complete set of critical safety functions, which are defined as a condition or action that prevents core damage or minimizes radiation releases to the public, needs to be fulfilled to ensure proper operator control of the event and public safety. The actions which ensure fulfillment of a safety function may result from automatic or manual actuation of systems, from passive system performance, from natural feedback inherent in the plant design, or when the operator follows guidance established in an event recovery guideline.

All critical safety functions are directed at mitigating an event and/or controlling radioactivity releases. These critical safety functions can be grouped into four major classes as follows:

- anti-core damage safety functions,
- containment integrity safety functions,
- indirect radioactive release safety functions, and
- maintenance of vital auxiliaries to support the other safety functions.

The anti-core damage safety function class contains five safety functions:

- reactivity control,
- RCS inventory control,
- RCS pressure control,
- core heat removal, and
- RCS heat removal.

The containment integrity function class contains three safety functions:

- containment isolation,
- containment pressure and temperature control, and
- containment combustible gas control.

The third safety function class has one safety function associated with it; indirect radioactive release. The purpose of indirect radioactive release control is to prevent radioactive release to the environment from sources outside containment including the spent fuel pool, the radioactive waste handling and storage facilities.

The fourth safety function class also includes only one safety function; maintenance of vital auxiliaries. Vital auxiliaries include instrument air needed for valve operations and electrical power and an ultimate heat sink.

2.15. Mitigation and control of severe accidents

A severe accident is one that involves appreciable core damage. The System 80+ Standard Plant Design represents a more resilient plant design not only to minimize the potential for core damage but also to moderate the severity of such an accident should one occur. This is the function of the containment and the systems that support it. A 200 ft diameter and 3.4 million cubic feet of free volume allow cost effective innovation to directly address severe accident concerns. Selected features include a reactor cavity that ensures coolability and retention of molten core debris, a passive cavity flooding system, and hydrogen igniters that operate independent of site power. An SDS is added to prevent containment failure caused by direct containment heating from high-pressure core melt ejection.

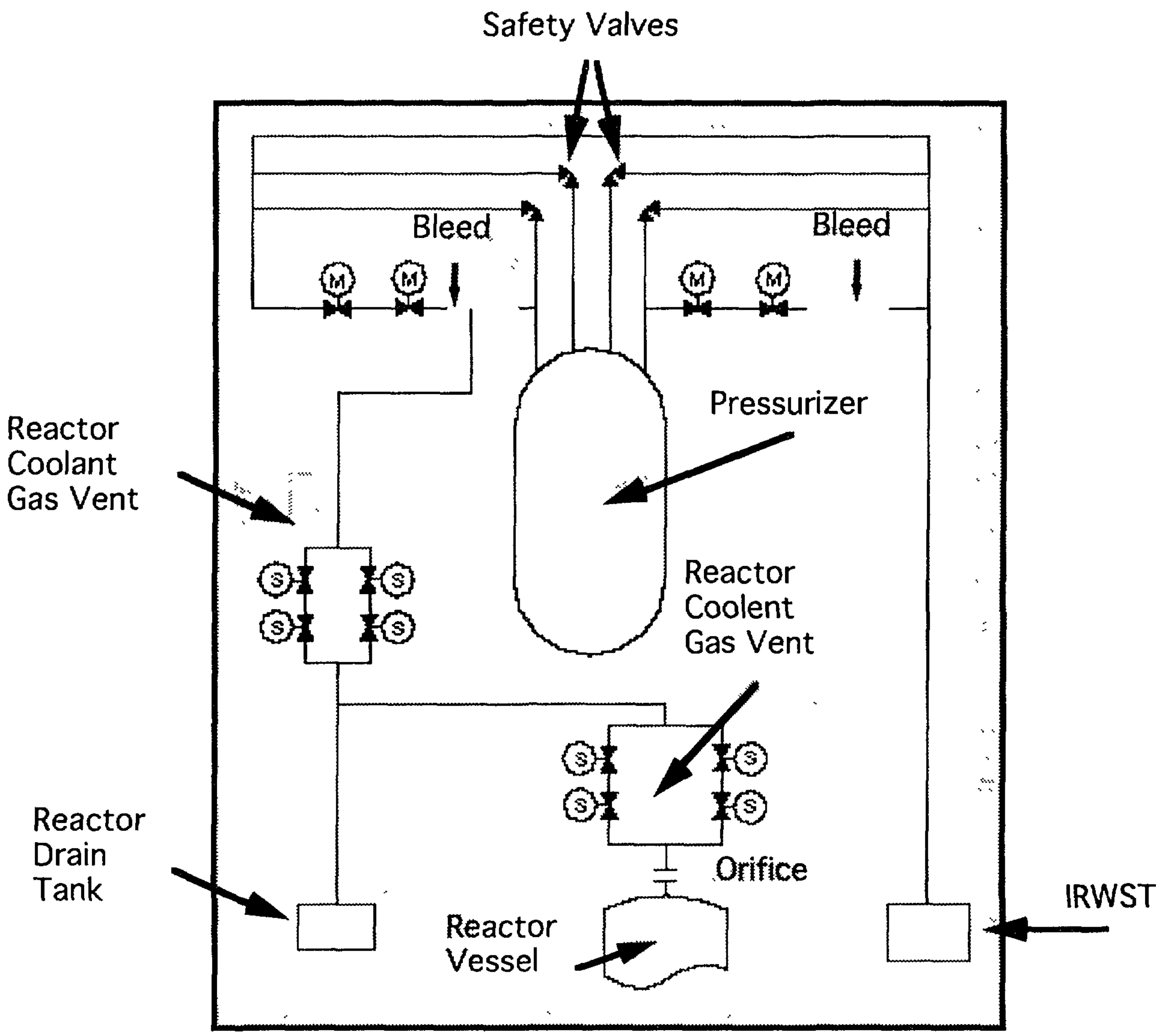


Figure 8: Safety Depressurization System

2.15.1. Reactor cavity and flooding system

The reactor cavity configuration is designed to prevent core debris transport and to provide coolability; it incorporates a gas and steam exit area greater than the area around the vessel, a collection volume twice the core volume, and a floor area greater than 0.02 square meter per MWt. The flooding system incorporates passive gravity flow from the IRWST to the cavity via a holdup volume.

2.15.2. Hydrogen control

The large System 80+ containment is designed to prevent hydrogen buildup by natural circulation and can passively accommodate a metal-water reaction of up to 75% of the core metal without exceeding a hydrogen concentration of 13% by volume. Igniters are provided to meet current NRC requirements to accommodate a 100% metal-water reaction and maintain hydrogen concentration below 10% by volume. The igniters can be powered from any one of four sources; normal off site power, on-site emergency diesels, batteries, and the combustion turbine generator.

2.15.3. Safety depressurization system

A dedicated SDS provides an alternate decay heat removal path through primary feed and bleed (Fig. 8). This offers a means to rapidly decrease pressure and thereby keep the core covered even when all feed water is lost. System pressure can be reduced from 2500 psia (17.2 MPa) to 450 psia (3.1 MPa) in less than 2 hours. Other benefits include normal decay heat removal and safety-grade depressurization during design basis events.

3. EXTENDED DATA LIST

Station Output

Rated thermal power of the reactor	3931 MWt
Net electrical output	1350 MWe

Fuel Assembly

Fuel material	Slightly enriched UO_2
Total quantity of UO_2	116.6 t (257,068 lb)
Number of fuel rods	236
Fuel rod, outside diameter	9.7 mm (0.382 in.)
Pellet diameter	8.25 mm (0.325 in.)
Clad material	Zircaloy - 4
Clad thickness	0.635 mm (0.025 in.)
Enrichment levels	3.3, 2.8, 1.9% w/o

Reactor Core

Number of fuel assemblies	241
Core height (active fuel)	3810 mm (150 in)
Core diameter (equivalent)	3658 mm (144 in.)
Number of control element assemblies	93
Absorber material	B_4C (48) Ag-In-Cd (20), Inconel (25)
Drive type	Magnetic jack
Number of fingers per assembly	4 or 12
Average fuel burn-up, first cycle	15,300 MWd/tU
first core	31,700 MWd/tU

Reactor Coolant System

Design pressure	17.2 MPa (2500 psia)
Design temperature	343.3°C (650°F)
Operating pressure	15.5 MPa (2250 psia)
Reactor inlet temperature	291°C (556°F)
Reactor outlet temperature	323.9°C (615°F)
Hot leg - I.D.	1065 mm (42 in.)
Cold leg - I.D.	760 mm (30 in.)
Flow rate (design minimum)	28 m^3/s (444,650 gal/min)
Active heat transfer area (core)	6590 m^2 (70,960 ft^2)
Average heat flux	602 kW/m^2 (183,600 $Btu/hr\text{-}ft^2$)
Average thermal output	18.1 kW/m (5.51 kW/ft)
Maximum thermal output	14.3 kW/m (12.6 kW/ft)

Reactor vessel

Inside diameter at shell	4630 mm (182.25 in.)
Overall height	15280 mm (601-5/8 in.)
Average wall thickness	229 mm (9 in.)
Min. SS clad thickness	3.17 mm (0.125 in.)
Material	SA-509

Diameter	
Shield building	65.8 m (216 ft)
Containment vessel	61 m (200 ft)
Concrete vessel thickness	0.91 m (3 ft)
Foundation slab thickness	3.05 m (10 ft)
Design pressure	0.365 MPa (53.0 lb/in^2)
Design temperature	143.3°C (290°F)
Free volume	$96.3 \cdot 10^3 m^3$ ($3.4 \times 10^6 ft^3$)

Turbine

Type	Tandem-compound, 1 high pressure 3 low pressure
Speed	1800 rev/min.
Boiler steam at inlet	
pressure	7.2 MPa (1044 psia)
temperature	287.8°C (550°F)

Condenser

Type	Three shell, three pass, divided water boxes
Design	2.473 MW (8.438×10^6Btu/hr)
Heat transfer surface	99,460 m^2 (1,070,600 ft^2)
Design pressure	
Shell	9.9/9.7/8.1 kPa (2.92/2.88/2.39 in. Hg)
Water box	1.73 MPa (251 psia)

Generator

Design	H_2 inner cooled
Speed	1800 rev/min.
Rating	1573 MVA
Terminal voltage	24 kV
Power factor	0.9
Frequency	60 Hz

Main transformer

Rated power	760 MVA
High voltage rating	230 kV
Low voltage	22.8 kV

Weight (incl. vessel head)	508 t (1,120,000 lb)
Reactor coolant pump	
Number of units	4
Type	Vertical, single stage centrifugal
Design pressure	17.2 MPa (2500 psia)
Design temperature	343.3°C (650°F)
Operation pressure	15.5 MPa (2250 psia)
Suction Temperature	291°C (556°F)
Design capacity	7 m^3/s (111,160 gal/min.)
Design head	114 mWG (374 ft)
Test pressure	21.5 MPa (3125 psia)
Motor type	AC induction single speed
Motor rating	8.95 MW (12,000 hp.) (cold)
Steam generator	
Number of units	2
Type	Vertical U-tube with integral moisture separator and economizer
Tube material	SB-163 NiCrFe alloy
Shell material, primary side	Low alloy steel clad with austenitic stainless steel
Shell material, secondary side	carbon steel
Shell side design pressure	8.3 MPa (1200 psia)
Shell side design temperature	298.9°C (570°F)
Shell side operating pressure	7.6 MPa (1100 psia)
Maximum moisture at outlet	0.25%
Test pressure, tube side	21.5 MPa (3125 psia)
Steam pressure at full power	6.9 MPa (1000 psia)
Steam temperature at full power	285°C (545°F)
Tube side design flow per steam generator	10,400 kg/s (82.9x10^{6}lb/hr)
Steam flow at full power per steam generator	1,100 kg/s (8.82x10^{6}lb/hr)
Pressurizer	
Internal free volume	68 m^3 (2400 ft^3)
Design pressure	17.2 MPa (2500 psia)
Design temperature	371.1°C (700°F)
Normal operating pressure	15.5 MPa (2250 psia)
Normal operating temperature	344.8°C (652.7°F)
Normal steam volume	34 m^3 (1200 ft^3)
Normal water volume	34 m^3 (1200 ft$^{3)}$
Installed heater capacity	2400 kW
Heater type	Immersion
Containment	
Type	Spherical steel containment shell, surrounded by reinforced concrete shield building

TECHNICAL INFORMATION ON DESIGN FEATURES OF THE SIZEWELL B PWR DESIGN

J. A. BOARD, M. V. QUICK
Nuclear Electric Plc.,
Knutsford, Cheshire,
UK

Presented by J. Bartlett

Abstract

The paper describes the Sizewell B PWR plant that is owned and operated by Nuclear Electric Plc. Its reactor design is a development based on well established PWR practices derived from the Westinghouse Electric SNUPPS (Standardised Nuclear Unit Power Plant System). The paper consists of three parts: - a general description of the plant concept and the safety approach; - a description of how the plant compares with the safety principles of INSAG-3 for 15 selected design areas; and - an extended data list. The general description describes the main features of the reactor plant and its safety systems, and presents the approach to nuclear safety. The second part discusses plant performance in the areas of: - plant process control systems; - automatic safety systems; - protection against power transient accidents; - reactor core integrity; - automatic shutdown systems; - normal heat removal; - emergency heat removal; - reactor coolant system integrity; - confinement of radioactive material; - protection of confinement structure; - monitoring of plant safety status; - preservation of control capability; - station blackout; - control of accidents within the design basis; and - mitigation and control of severe accidents. The third part, finally, presents data related to the power plant as a whole, data on reactor core and fuel, on the reactor coolant system, the reactor pressure vessel, coolant pumps, steam generators, pressurizer, accumulators, and coolant pipes, on charging and injection pumps and other system pumps, on the turbine, the condensate, main and auxiliary feedwater, and circulating water pumps, and on the containment, including the refuelling water storage tank.

1. GENERAL DESCRIPTION AND SAFETY APPROACH

1.1. Reactor design

1.1.1. Outline

The Sizewell B power station consists of a single 4-loop pressurised water reactor of 3411 MW thermal output linked to two turbine-generators giving a net electrical output of 1183 MW. The plant that is owned and operated by Nuclear Electric, the electrical utility operator of nuclear power stations in England and Wales, was started up in September 1994.

The reactor design is a development based on well established PWR practices, being derived from the Westinghouse SNUPPS (Standardised Nuclear Unit Power Plant System) design.

1.1.2. Fuel and core

The fuel is low-enriched uranium oxide clad in zircaloy: 236 fuel rods form a fuel assembly, and there are 193 fuel assemblies, supported by stainless steel structures in the core (see 2.4). Control rods forming rod cluster control assemblies (RCCAs) can be inserted into the core in interstitial spaces within certain of the fuel assemblies, and they are grouped into a number of "banks" for reactor control and for shutdown (see 2.5).

1.1.3. Reactor coolant system

The core is cooled and moderated by water at a pressure of 15.5mpa. The reactor coolant system (RCS) comprises the Reactor Pressure Vessel (RPV), four centrifugal reactor coolant pumps, four vertical steam generators with the primary circuit passing through an inverted U tube bundle, a pressuriser and linking pipework. The reactor coolant boundary is designed, constructed, inspected and tested to a very high standards to give a high level of integrity (see 2.8). There are a number of systems connected to the reactor coolant system. These include the residual heat removal system (RHRS) for removing reactor decay heat when the system temperature has fallen below the level when heat can be removed via the steam generators and feed and steam systems.

The reactor design incorporates a considerable degree of redundancy and diversity in systems providing safety functions, including the systems for rejecting decay heat (see 2.7).

1.1.4. Reactor protection system

The reactor protection system (RPS) which initiates reactor trip and particular engineered safety features in response to fault conditions, comprises two diverse systems, the primary protection system (PPS) and the Secondary Protection System (SPS), based upon different operating principles (see 2.5).

1.1.5. Engineered safety features

The engineered safety features comprise:

i. the containment system, comprising a primary and secondary containment together with supporting systems for cooling aerosol removal, containment isolation and hydrogen control.

ii. the emergency core cooling systems, which, in the event of a loss of coolant accident (LOCA) can inject borated water into the reactor coolant system, to maintain adequate core cooling and to prevent core damage (see 2.2).

iii. the auxiliary feedwater system (AFWS), which can provide feed to the steam generators to remove decay heat in the case of failure of the normal feed system (see 2.2).

iv. the emergency charging system (ECS), able to provide seal injection to the reactor coolant pump seals, and make-up water to the reactor coolant system, if the normal system (the Chemical and Volume Control System, CVCS) providing these functions should fail.

v. the emergency boration system (EBS), a diverse means of reactor shut-down which can rapidly inject borated water into the reactor coolant system in the event of inadequate control rod insertion during a reactor trip or in the event of certain cooldown faults (see 2.5).

The above systems are supported by a four train electrical system, comprising the main electrical system linked to the offsite supplies, and the essential electrical system which can be supported by on site diesel generators.

1.1.6. Control and instrumentation

The control and instrumentation systems provide means by which the plant and processes involved in the normal operation of the station and in post-fault conditions, can be safely controlled. The main control room is the centre from where the plant operators are able to start up, operate and shut down the reactor. It is from here that the operators would normally monitor plant operation but in the event of this main control room being uninhabitable, an alternative auxiliary shutdown room is available which allows for the achievement of hot shutdown. Longer term activities associated with the maintenance of the shutdown state would be achieved by local to plant operations, ie operations carried out local to the particular plant items.

The station automatic control systems comprise several control loops which between them control such parameters as reactor power, primary coolant inventory and pressure and turbine load.

The reactor itself is controlled by the negative moderator temperature coefficient and fuel temperature coefficient (doppler) in conjunction with movement of the rod control cluster assemblies and changes in the boron concentration. Control rod motion is used mainly to accommodate load changes and for start-up and shutdown. The boron concentration is adjusted mainly during shutdown and start-up and to compensate for fuel burnup and the accumulation of fission products.

1.1.7. Refuelling

The reactor is refuelled at shutdown, involving the removal of the reactor pressure vessel head. The cavity above the vessel and the route to the port where the fuel assemblies pass through the containment is flooded with water during this process. Spent fuel assemblies remain in the fuel storage pond for a significant time during which their decay heat level decreases, before being transported off the site in fuel transport flasks.

1.2. Nuclear safety approach

1.2.1 Overall targets

The nuclear safety strategy which has been adopted for the Sizewell B station rests on five fundamental principles. These principles are applied to all Nuclear Electric's stations and are also the fundamental principles adopted by the UK Nuclear Installations Inspectorate in assessing the safety of nuclear plant for licensing. They are as follows:

i. No person shall receive doses of radiation in excess of the statutory dose limits as a result of normal operation.

ii. The exposure of any person to radiation shall be kept as low as reasonably practicable.

iii. The collective effective dose equivalent to operators and to the general public as a result of the nuclear installation shall be kept as low as is reasonably practicable.

iv. All reasonably practicable steps shall be taken to prevent accidents.

v. All reasonably practicable steps shall be taken to minimise the radiological consequences of any accident.

These principles are embodied in guidelines used in the design and development of the plant. These guidelines incorporate certain numerical design targets to ensure the safety principles are achieved.

With respect to the risk arising from accidents, the level of acceptability for fatal risks to individual members of the general public has been taken as 10^{-6} per year. That is, a level at which the risk of death to any individual member of the general public, arising from the operation of the station over a period of one year, should not exceed one in a million. This is consistent with public judgements of acceptable risk levels.

Implementing the fundamental principles involves the approach to design, construction and operation to ensure that during normal operation, doses to operators and the public are As Low As Reasonably Practicable (the "ALARP" principle), that faults are prevented from occurring as far as reasonably practicable, and if a fault should occur, the consequences should be limited as far as is reasonably practicable. The approach to safety analysis requires that faults are systematically considered and adequate safety provisions are shown to exist in each case.

In addition, consideration has to be given to ensuring that decommissioning of the station can be carried out safely and efficiently.

1.2.2. Radiological safety during normal operation

The basic target relating to restriction of the dose rates to the personnel is an annual effective dose equivalent of 10 mSv. In addition, the collective station dose equivalent should not exceed 2 manSv/yr per GWe installed capacity.

Radiation doses to the public are principally from liquid and gaseous effluents. Authorizations for discharges are granted by the relevant Government departments. Dose targets will be set at a level of 1/30 of that recommended by the ICRP for the general public.

On Sizewell B, occupational doses to personnel are controlled by measures including reducing cobalt levels in the core and reactor coolant systems, reducing transport and deposition of corrosion products by appropriate water chemistry control, minimising fuel clad failures and careful failed fuel management, suitable radiation shielding, and minimisation of contamination sources and providing facilities for decontamination. In addition, the layout of the station and control of access to radiation and contamination controlled areas is organised to reduce radiation exposure, and to monitor and control liquid and gaseous effluents. There are provisions to treat liquid effluents as necessary in the liquid radwaste system.

The gaseous radwaste system provides for adsorption of halogens, filtration of particulates and the hold-up of noble gases arising from the gaseous fission products of purged from the primary coolant system.

Dedicated heating, ventilation and air-conditions systems are used to collect, filter and discharge the airborne contamination arising from controlled areas via high level vent stacks.

Continuous monitoring and sampling of discharges ensure that authorised levels are not exceeded.

1.2.3. Avoidance and mitigation of faults

In general, faults are avoided by adopting the following measures:

i. A well established design.

ii. Well established and controlled approaches to the design and construction of the plant. These approaches include the categorisation of components and structures according to their safety significance, the use of established codes and standards, consideration of the range of operating conditions in the specification of the plant, the choice of appropriate materials, the qualification of components against specified operating conditions and the adoption of particularly high standards and requirements for components whose failure is claimed can be discounted (see 2.8).

iii. Commissioning, pre-service and in-service testing of the systems and plant.

iv. Organisational and management structures and arrangements, including procedures and documentation, aimed at ensuring that well controlled and safe operational practices are implemented.

v. Suitable protective measures.

vi. Quality assurance practices throughout the design, construction, commissioning and operation of the plant.

In addition to these measures, the mitigation of faults which do occur is facilitated by:

a. The systematic and comprehensive identification of potential faults which are then taken account of in the design.

b. The design and operation of the plant in ways that limit the severity of faults and their consequences.

c. The identification of requirements needed to achieve successful mitigation.

d. The provision of reliable safeguards equipment, incorporating redundancy and diversity as appropriate. (NB - Sizewell B incorporates more extensive diversity provisions than general on contemporary plants. (see sections 2.5, 2.7).

e. The adequate preparation of staff, by the provision of training and documentation, to enable them to deal effectively with faults.

f. The provision of pre-planned actions to cover emergency situations.

g. The adoption of provisions to allow plant recovery which do not result in unacceptable doses to operators or the public.

1.2.4. Fault analysis

The fault analysis includes both deterministic analysis methods and a very extensive probabilistic assessment. The fault analysis considers a very wide range of initiating faults.

The design basis assessment demonstrates the robustness of the design to tolerate faults by demonstrating that certain fuel and plant limits are not exceeded, while taking account of some deterministic criteria such as the single failure criterion. These limits are set conservatively to ensure the overall integrity of the system of barriers to the release of radioactivity- the fuel and its cladding, the reactor coolant system boundary, and the containment is maintained. A further limit is set on radiological dose to the public, at a level so that countermeasures to the public are unlikely to be required, the so-called Emergency Reference Level, (ERL), generally 100mSv (10 rem) whole body dose, 300mSv thyroid dose.

In addition, targets are set for the summated frequencies of fault sequences giving rise to doses to the public in given ranges, greater frequencies being permitted for lower doses.

Targets are also set for the frequency of accidents giving releases beyond those acceptable within the design basis. The maximum frequency for any single accident type is 10^{-7} per year, and the summated frequency target for beyond design basis accidents is 10^{-6} per year.

The Probabilistic Safety Assessment (PSA) has taken account of a wide range of conditions, including risks from common-mode failures, at reactor shut-down and from internal and external hazards. PSA levels 1, 2 and 3 have been performed, which includes an assessment of the ability of the plant to mitigate the releases from severe accidents, including degraded core conditions. These assessments generally indicate compliance with the numerical targets set, and that there is no "threshold" of a very large increase in releases just below the target frequencies.

1.2.5. Hazards

The extensive analysis of internal and external hazards has lead to a high degree of redundancy and segregation to protect against the effects of fires, pressurised component failures, missiles or flooding and design against seismic hazards.

The site specific Safe Shut-Down Earthquake (SSE) is 0.14g Zero Period Acceleration. However, most of the components and systems have in fact been designed and qualified at significantly higher levels (typically 0.25g), and it has been demonstrated that the plant has significant seismic margins above the SSE.

The risk from aircraft crashes has been assessed, and for the type of aircraft crash (a light plane) shown to exceed the target frequency of 10^{-7}/yr, the containment structure combined with the redundancy and segregation of systems provide adequate protection. Similar features, in conjunction with turbo-generator axes orientation approximately in line with the reactor building, ensure an adequately low risk from turbine generated missiles.

2. DESCRIPTION OF 15 SPECIFIC DESIGN AREAS AS SELECTED FROM INSAG-3

In the following sections the reference to INSAG-3 is put in parenthese after each heading.

2.1. Plant process control systems (4.2.2.1)

The station's data processing and control facilities allow for the manual and automatic control of the plant. They collect and display data relating to the state of the plant in the main control room, and where appropriate, in the alternative auxiliary shut-down room. The control rooms are designed on ergonomic principles, and the overall control and instrumentation system takes account of human factors engineering to minimise the likelihood of human-errors in operating the plant.

The reactor is generally controlled automatically to ensure that parameters remain within the designed operating ranges which are less extreme than the reactor trip set points. This high integrity control system incorporates redundancy, segregation, fault tolerance and self-test features. Where the control system uses parameters derived from detectors common with the Reactor Protection system, optical links are used to prevent any control system faults affecting the protection system.

The part of the station control system relating to the control of the turbines is implemented within the turbine governors. The turbine load controller, which acts on the turbine governor control valve, can be set to operate for base load operation (the preferred mode) or for grid frequency control.

Changes in the governor valve position reflect back into the reactor primary system and secondary system parameters. The station automatic control system acts to control the reactor by the following sub-systems:

i. The reactor coolant temperature control system maintains the primary coolant temperature at its demand value during normal operation, and restores it to that value following transients. It does this by adjusting the position of the appropriate control rod bank.

ii. The pressuriser pressure control system - limits the reactor coolant system pressure variations during all modes of operation, and minimises the likelihood of discharges through the pressuriser relief valves or safety valves, or of reaching the reactor trip set-point for pressure. The control system measures the primary coolant pressure, and acts by energising the electric heaters in the pressuriser, or actuating the pressure sprays.

iii. The pressuriser level control system - regulates the charging flow valve in the Chemical and Volume Control System (CVCS) to achieve the desired level in the pressuriser.

iv. The steam generator level control system - controls the level of water in each of the four steam generators at all power levels between 5% and 100% of full load, by four independent control loops acting on the feedwater regulator valves.

v. The feed-pump speed-control system - acts on the feed pumps (normally two 25% pumps out of three in each of the two feed trains drawing from the two de-aerators), to maintain the correct pressure differential between the main feed header and the main steam header, and to ensure that the individual feed train flows reflect the individual turbine loads.

vi. The Steam Dump Control System - enables excess steam production to be dumped through dump valves. The aim of dumping steam in a controlled manner is to minimise the transient effects on the reactor during startup, hot shut-down, cool down or sudden large transient reductions in steam demand.

2.2. Automatic safety systems (4.2.2.2)

Sizewell has highly reliable automatic safety systems to safety shutdown the reactor, maintain it in a safe condition and limit the release of radioactivity which might occur if operating conditions exceed certain setpoints. This reliability is provided by systems having appropriate redundancy, diversity and independence, whose performance has been assessed for a wide range of initiating fault conditions by comprehensive fault analysis. The fault analysis demonstrates that the integrity of the system of barriers to radiological release (fuel matrix and clad, Reactor Coolant System boundary, and the containment system) is retained in its entirety, or with sufficient barriers remaining to ensure release targets are met. The fault analysis ensures the integrity by showing that conditions of pressure, temperature etc., remain within suitable limits for the fuel, for pressurised components, for the containment etc. For pressurised components, ASME limits are used (ASME levels A, B, C & D), the limits being more stringent for the more frequent faults. The analysis shows that deterministic criteria such as the single failure criterion are met, as well as probabilistic targets (see 1.2.4).

The Engineered Safety Features (described in 1.1.5) comprise:

a. the Containment Systems (primary and secondary containment with filtered vented interspace), containment isolation and containment spray system (which can scrub out radioactive aerosols and also provide containment cooling), and the combustible gas control system.

b. the Emergency Core Cooling System, comprising a system able to inject borated water adequate to maintain core cooling in the event of loss of coolant accidents. This is a four-way redundant system of pressurised accumulator tanks, and pumps able to deliver water to suitable points in the Reactor Coolant System.

c. the Auxiliary Feedwater System - a system with redundant and diverse pumps (two electric drive, two steam turbine driven) able to provide feed to the steam generators to remove decay heat in the case of failure of the normal feed system.

d. the Emergency Charging System - able to provide seal injection to the reactor coolant pumps and to provide boration and coolant make-up, in the event of failure of the Chemical and Volume Control System.

These systems which are safety classified, are supported by electrical and control and instrumention of commensurate reliability, the safety categorisation of the support systems being, in general, the same as the relevant engineered safeguard system.

The systems for initiating the actions of engineered safety features are themselves diverse and incorporate redundancy.

Diversity has been provided for functions required to protect against initiating events having a frequency greater than 10^{-3} per year.

2.3. Protection against power transient accidents (4.2.3.1)

The reactor has a negative moderator temperature coefficient and a negative fuel temperature coefficient (Doppler), ensuring stable operation and stable response to normal transients. The reactor control system (2.1) enables the reactivity to be controlled safely under all conditions, by means of solid control rods (see 1.1.2), together with adjustment of the concentration of boron in the primary circuit by the Chemical and Volume Control system.

If certain parameters exceed their trip limit valves, the reactor protection system (RPS) releases control rods in the RCCAs under gravity into the core, or initiates the Emergency Boration System (2.5) in case of failure of the normal rod shut-down system. These trip limits are set below the valves at which safety limits for fuel or reactor coolant system boundary would be exceeded, so any subsequent transient remains within these safety limits. The reactor protection system incorporates two independent diverse systems, the Primary Protection System (PPS) and the Secondary Protection System (SPS). The sensors relevant to power transient accident protection that feed into the RPS include:

- Rod Cluster Control Assembly (RCCA) position measurement
- Ex-Core neutron flux channels
- Nitrogen-16 gamma detectors.

The PPS and SPS process the measured plant parameters which enables certain derived parameters such as linear power density or Departure from Nucleate Boiling Ratio (DNBR) to be calculated.

The likelihood of reactivity accidents due to incorrect withdrawal of RCCAs is minimised by the sub-division of the RCCA control groups into a number of different "banks", with strict control over the sequence in which they can be withdrawn, and with mechanical self-limitation of the speed of withdrawal. There are three banks for reactor control and six banks for reactor shut-down. Burnable poisons limit the requirement for excessive reactivity hold down by the control rods or coolant boration during the life of the first fuel charge.

The fault analysis considers the limiting case of ejection of a RCCA from the core to demonstrate the safety of the reactor in this extreme event.

During all phases of power operation, the RCCA shutdown banks are fully withdrawn from the core. As shut-down, the reactor is held subcritical with all the control and shut-down banks of RCCAs fully inserted, and the boron concentration of the reactor coolant adjusted to achieve an adequate shut-down margin.

During refuelling, the majority of the RCCAs remain in the core, the refuelling pool above the reactor vessel is filled with borated water, with an adequate reactor shut-down margin ensured by the appropriate concentration of boron content in this water and in the reactor coolant, even if all control rods were removed.

The general provisions against external hazards, and the high degree of attention given to human factors in the design, minimise the probability of reactivity induced accidents due to external events or human errors.

2.4. Reactor core integrity (4.2.3.2)

The design of the reactor core is based upon extensive experience of development and operation of similar cores.

The fuel rods (Zircaloy clad, UO_2 pellets) are supported and located within Fuel Assemblies, 264 fuel rods per assembly on a 17 x 17 square array. The assembly structure is a skeleton comprising a top and bottom nozzles, 24 connecting guide, thimble assemblies, an instrumentation tube and eight stiffening grid assemblies. The top and bottom nozzles provide flow guidance and form the structural element at the top and bottom of the assembly. The eight grid assemblies are spaced at intervals along the length of the assembly, maintaining the correct lateral spacing of the fuel rods while allowing for differential thermal expansion and irradiation induced growth of the rods, thus avoiding distortion of the skeleton.

The reactor core contains 193 fuel assemblies. These are supported and located by the reactor internal structures. There is a lower internal assembly, of which the two main features are the cylindrical core barrel and the lower core support, which in turn locate the lower core plate. This plate locates the bottom of the fuel assemblies and guides coolant into them. There is also an upper internal assembly which locates the top of the core assemblies and provides guide tubes for the rod cluster control assemblies. These guide tubes and the guide thimbles prevent flow induced movement of the RCCAs. The whole core structure locates the core components in a manner to prevent unwanted movements or vibrations. The relatively low coolant temperature rise through the core (approx. 30°C) implies relatively small relative-expansion problems.

The core structure is seismically qualified to a level significantly above the Safe Shut-down Earthquake for the site.

The fuel rods, the assemblies and core components are manufactured to high quality standards. The functional requirements set and the reactor operating parameters are such that during operation, fuel and core components remain intact, although a small number of random failures of fuel rods cannot be precluded, but these must be within the cleanup capability of the CVCS. The level of radioactivity of the coolant is monitored to ensure they remain within the levels set by the Technical Specifications. The provisions for safe protection and safeguards against faults are such that for "frequent faults" (taken as greater than approx 10^{-3}/yr) fuel and core components remain intact, although again a small number of random failures cannot be precluded. For infrequent faults ($<10^{-3}$/yr) the fuel remains in a coolable geometry and the reactor remains capable of being shutdown safely. Any fuel clad failures that occur, do not lead to significant radiological releases.

2.5. Automatic shutdown systems (4.2.3.3)

The reactor trip and shutdown systems incorporate redundancy and diversity to provide a high degree of reliability.

Shutdown can be initiated when certain parameters go outside their set trip valves by the Primary Protection System (PPS) or the Secondary Protection system (SPS), which are based on diverse principles. The reactor shutdown by insertion of neutron absorbing material into the core can be achieved by solid rod cluster control assemblies which can be dropped into the core in the event of a reactor trip, or alternatively for "frequent" faults (ie greater than 10^{-3}/yr) also by an Emergency Boration System (EBS).

The primary protection system uses microprocessor based technology to provide tripping for all faults within the design basis.

The secondary protection system uses technology of which there is extensive experience in the UK, using trip amplifiers, pulse to d-c convertors, and solid state magnetic logic. This system is totally diverse from the PPS. Both systems are fully independent of the normal reactor control system. Where detectors are used to provide parameters for both the control system and the protection system, optical links are used to prevent any possible interference in the correct functioning of the protection system.

The rod control cluster systems are grouped into banks, three for reactor control and six for shutdown, which can only be withdrawn in a pre-determined sequence and at a limited rate to limit the rate of reactivity addition.

The Emergency Boration System consists of four boric acid storage tanks with discharge pipework normally isolated by valves connecting to the reactor coolant system cross-over legs (between the steam generators and the pumps) and return pipework connecting to the cold legs. Operating the valves injects the boric acid into the reactor coolant system under the influence of the reactor coolant pump pressure differential.

The diversity provided in reactor trip systems and reactor shutdown system give a very high degree of reliability. For this reason, it is considered that Anticipated Transients Without Scram (ATWS) do not contribute significantly to the overall risk and need not be analysed.

2.6. Normal heat removal (4.2.3.4)

The normal heat removal path from the core, by means of the reactor coolant system to the steam generators (section 1.1.3) relies at power for circulation upon the reactor coolant pumps, powered by the offsite power supplies. The heat is normally removed from the steam generators by the steam systems, feeding the two steam turbines. Exhaust steam is condensed in the condensers, and is returned via the condensate polishing plant, the deaerators and the feed train to the steam generators. There are three 50% feed pumps associated with each turbine generator.

Following a normal reactor trip, the reactor coolant pumps continue to operate, and the feed pumps operate feeding the steam generators via a small-bore system to provide a suitable quantity of feed for the conditions. In the case of loss of normal power supplies, the reactor coolant pumps would coast down and stop, the core decay heat being removed by primary coolant flow under natural convection. In case of loss of the main feedwater system (due to loss of normal power supplies or for other reasons), the Auxiliary Feed System is brought into service. This has two redundant electric motor driven feed pumps that can be powered by the Diesel Generator backed Essential Electrical system, and two steam turbine driven feed pumps providing a diverse means of feed in case of total loss of electric supplies.

Heat removal via the steam generators provides decay heat removal until the reactor pressure and temperature fall to levels where this route is no longer effective, when the Residual Heat Removal System (RHR) takes over.

A steam dump system allows the steam to bypass the turbines directly to the condensers or to be dumped to atmosphere in the case of a turbine trip, thus reducing the likelihood of an inadvertent reactor trip due to this cause.

2.7. Emergency heat removal (4.2.3.5)

For most intact circuit fault conditions, the heat removal from the core is via the steam generators, using the normal feed and steam systems, or the auxiliary feedwater system and steam dump facilities described in II.6 above. In the event that the main condenser is unavailable, steam will be dumped either by the atmospheric dump valves or by the power-operated relief valves.

The Residual Heat Removal System (RHRS) which operates when the primary system pressure and temperature are low, rejects heat via the closed loop Component Cooling Water System. This, in turn, rejects heat to the sea water Essential Service Water System, or in the event that this should fail, to the Reserve Ultimate Heat Sink (RUHS) which is air-cooled. The RUHS is seismically qualified and is the heat sink used after a seismic event.

In the case of the loos of coolant accidents (LOCAs), core cooling is maintained by the Emergency Core Cooling Systems (ECCS), able to inject water into the reactor cooling system at a sufficient rate to preclude core damage in the event of the largest pipework rupture (see 2.2).

The redundancy and segregation within these systems, the high integrity of initiation systems and power supplies, and the diversity provided for protection against frequent fault ($>10^{-3}$/yr) ensure a very high degree of reliability of emergency heat removal.

2.8. Reactor coolant system integrity (4.2.3.6)

The materials used for pressure-retaining applications in the reactor coolant pressure boundary components have been selected from those specified in the American Society of Mechanical Engineers (ASME) Code. In some cases, additional requirements or additional restrictions have been specified beyond those quoted in the appropriate ASME materials specification.

Ferritic steel has been used in the fabrication of many of the reactor coolant system components. Where surfaces are exposed to the primary coolant these are clad with corrosion resistant alloys, austenitic stainless steels and nickel-chromium-iron alloys.

For ferritic materials in order to minimise the risk of cracking associated with welding and to ensure adequate toughness all welding and cladding operations were conducted using procedures qualified according to the rules of the ASME Code, Sections III and IX as a minimum. Manufacturing processes have been controlled so that adequate fracture toughness is achieved in all parent materials and welds.

The welding of austenitic stainless steel has been controlled to minimise the occurrence of hot cracking in the weld. The susceptibility of stainless steel welds to hot cracking has been effectively removed by ensuring a minimum delta ferrite content during solidification. Each full welding process has been subjected to a quality audit.

Fabrication and installation welds in austenitic steels were inspected using ASME III non-destructive examination methods supplemented by ultrasonic inspection. Production welding was monitored to verify compliance with the limits for the process variables.

The reactor coolant water chemistry has been selected to achieve minimal corrosion. Routinely scheduled analyses of the coolant chemical composition will be performed to verify that the reactor coolant chemistry meets the specifications. The Ph control chemical utilised is lithium hydroxide monohydrate, enriched in the lithium-7 isotope to 99.9%. This chemical is chosen for its compatibility with water chemistry of borated water, and stainless steel, zirconium, and nickel-based alloy systems.

Components forming the reactor coolant pressure boundary have been designated safety category 1, safety class 1 and have been designed in accordance with the ASME III Code. This has ensured that very high standards have been applied in design, materials selection, fabrication, testing and inspection. The components have been procured from established and experienced suppliers.

Consideration has been given, in the design and analysis of components, to the range of internal and external hazards discussed in 3.6 above. They have been designated seismic category 1 and as such are required to maintain their integrity during the Safe Shut-Down Earthquake.

The loading conditions imposed upon the reactor coolant system during normal operation, anticipated operational transients and fault conditions have been analysed. The design loadings in the reactor coolant system pressure retaining components meet the ASME III code limits, viz:

Normal operation - (condition I) - Service level A
Incidents of moderate frequency (Condition II) - Service level B
Infrequent faults (Condition III) - Service level C
Limiting faults (Condition IV) - Service level D

This analysis demonstrates that the reactor coolant system integrity will not be jeopardised by the range of plant conditions encountered.

In addition to the controls applied to materials and processes discussed above, a programme of inspection was applied during manufacture to ensure that the components which forms the pressure boundary were free from initial defects which might compromise their integrity during their planned life. A rigorous programme of in-service inspection is applied to ensure that no defects arising from operation remain undetected based on the ASME XI code.

The reactor coolant system is subjected to a hydrostatic overpressurisation test of 1.25 times the design pressure prior to entering service. Hydrostatic tests of the reactor coolant pressure boundary are conducted at or near the end of each inspection interval (10 years) and system leakage tests are carried out prior to start-up following each reactor fuelling shutdown.

For certain components, the range and depth of measures which contribute to the achievement of integrity are such that gross mechanical failure can be discounted. For the reactor coolant system this applies to the following components:

- reactor pressure vessel;
- steam generator primary and secondary shell, including tubesheet;
- pressuriser shell;
- reactor coolant pump casings and motor flywheels;
- reactor internal core barrel;
- the vessel, steam generator and pump supports.

The range of measures adopted was as follows:

- the use of a proven design for the plant;
- the application of very high standards of materials selection, design, manufacture and construction;
- implementation of high standards of quality assurance;
- in-process, pre-service and in-service inspections;
- control of operating conditions;
- in-service plant condition monitoring.

An example of the additional steps taken for these components is illustrated by the approach to in-process inspections. In all cases the non-destructive examination methods adopted reflect the best of world experience. The equipment, procedures and operators were independently validated: this involved practical tests on samples which adequately represented the component geometry and relevant defect types. The validated inspection defect size is that which the validation exercise has shown will be detected, positioned and sized, reliably by the procedures, equipment and operators employed.

The inspection methods were developed to contain redundant and diverse elements such that a very high level of confidence has been achieved. Further, the implementation of all inspections was controlled within the project quality assurance programme and was witnessed by an independent inspection agency.

For these components for which gross mechanical failure is discounted, a fracture assessment has been conducted. The results from this showed an adequate margin in the ratio of the critical defect size to the end-of-life defect size. In the reactor pressure vessel, longitudinal welds in the region of high neutron flux levels are avoided by the use of ring forgings for the cylindrical shell of the vessel.

2.9. Confinement of radioactive material (4.2.3.7)

The reactor coolant system and certain connected systems are located within containment system. This consists of a large (90,000m^3) primary containment structure of prestressed concrete with a liner, which is surrounded by a secondary containment which includes those buildings adjacent to the primary containment and a reinforced concrete enclosure surrounding the primary containment. The interspace between the primary and secondary containments is maintained at a sub-atmospheric pressure following a loss of coolant accident or other release of radioactivity into the primary containment, by an emergency exhaust system, which discharges through filters to the stack. The primary containment is cylindrical with a hemispherical domed top, designed (design pressure 0.345MPa) and constructed to the ASME III code, as a Safety Category I structure to withstand with a significant margin, the highest pressure that can occur in any design basis accident.

The pipework penetrations, and man and equipment access hatches are designed to the same standards of integrity as the containment structure. The containment has been tested during commissioning to demonstrate its strength and leak tightness and will be tested at intervals during the station life.

Additional systems are provided to ensure the containment function is effective during accident conditions. These include:

i. The containment isolation provisions - which can rapidly isolate those process piping systems which penetrate the containment structure which are not required as part of the operation of relevant safeguards equipment. Those pipework systems on the containment atmosphere have at least two valves in series, generally one inside and one outside the primary containment wall. The operation of the isolation valves is initiated by the Engineers Safety Feature Actuation System (ESFAS) on receipt of signals indicating a LOCA or other relevant condition. These are high integrity systems to prevent a significant risk from containment bypass accidents.

ii. The reactor spray system, which can spray borated water into the containment to assist in scrubbing out aerosols, and to provide cooling to reduce the containment pressure after a pipe break accident. This is a two train system, but having the possibility of making use of the RHRS pumps by re-alignment in the case of loss of the spray system pumping capacity. The system initially draws water from the Refuelling Water Storage Tank, and later from the containment sumps in a recirculation mode.

iii. The fan coolers, in conjunction with the spray system, provide containment atmosphere mixing and heat removal from the containment to the Component Cooling Water System. In addition, there is a system for hydrogen control incorporating re-combiners, to prevent hydrogen levels reaching concentrations which could combust.

Fault Analysis for design basis accidents show that these stringent targets for radiological releases should be met. The containment has large margins which will also give significant protection in the case of severe accidents (see 2.15).

2.10. Protection of the confinement structure (4.2.3.8)

An extensive assessment has been made of the resistance of the containment design to Severe Accidents and it can be shown that the containment provides a valuable measure of risk reduction in such accidents. Factors include the very large (90,000 m^3) rugged double containment whose performance in severe overpressure conditions has been demonstrated in model tests, acceptable hydrogen concentrations (less than 10%) due to the large containment volume, and an ability to cool and retain core debris by flooding the reactor cavity. Diverse means of maintaining containment cooling are available, including systems that do not require any active components inside the containment in Severe Accident conditions.

In conjunction with the low probability of the occurrence of severe accidents, the objectives of achieving a very low risk to the public are achieved.

2.11. Monitoring of plant safety status (4.2.3.9)

Key information which enables the operations staff to assess and maintain safety at all times is presented in a clear and concise manner. The information is available from an appropriate mix of discrete instrumentation and computer based visual display units. The safety information display system permits monitoring even in the event of a failure of the distributed computer system.

The displays and alarms indicate all information relevant to normal plant operation. In addition to basic parameters, a distributed computer system acquires and processes data from the other station control and data acquisition systems in order to provide a graphic information display system consisting of dynamically updated visual display units. The system provides a number of specialised nuclear related calculations and displays, approach to trip alarm calculations and engineered safety features actuation alarm processing.

The distributed computer system provides a greater degree of sophistication of man-machine interface than that provided by the other display facilities by providing animated mimics, trends and bar graphs, and by supporting operational staff in their duties by providing task-related processing and display facilities.

Monitoring facilities are provided in the main control room to allow the following monitoring functions to be carried out:

- Direct post-fault monitoring of safety functions.
- System monitoring of equipment within a system whose state contributes to the achievement of a safety function.
- Limits of operation monitoring to ensure that the station remains within safe limits.
- Condition monitoring and recording related to equipment health and performance degradation. Although facilities exist in the main control room,this function would normally be carried out from the technical support centre.

Alarms are provided in the main control room to alert the operating staff to the occurrence of faults, hazardous situations, violations of operating limits, unauthorised entry into restricted areas and incidents which may jeopardise public or operator safety.

Loose parts monitoring and core vibration monitoring is provided. Post-fault neutron flux measurement is provided by the protection system source range detectors.

Special instrumentation systems include fire detection, seismic instrumentation, radiological protection instrumentation, health physics instrumentation.

The reactor coolant pressure boundary forms one of the barriers which prevent radiological release. Detection of system leakages is therefore of major importance.

Leakages from the reactor coolant pressure boundary may occur into the reactor building, into the secondary side of the steam generators, or into other systems connected to the reactor coolant system.

The following methods are available for detecting leakage into the reactor building:

- The reactor building atmosphere radiation (gamma) monitoring.
- The reactor building atmosphere contamination (particulate iodine gaseous activity) monitoring.
- The reactor building sump level and sump flow monitoring.
- The reactor building fan cooler condensate standpipe level monitoring.
- The reactor building atmosphere humidity monitoring.

The secondary side parameters which indicate steam generator tube leakage are:

- High nitrogen-16 or gross gamma activity in the steam lines.
- High condenser off-gas activity.
- High steam generator blowdown process activity.
- High nuclear sampling system steam generator activity.

Leakage into those systems that are connected to the reactor coolant system is detected by increases in the auxiliary system level, temperature and pressure indications or by lifting the relief valves.

2.12. Preservation of control capability (4.2.3.10)

The main control room provides the principal interface between operating staff and the systems necessary for the safe and effective operation of the station. The auxiliary shutdown room, together with equipment local to plant, provides an additional interface in situations when the main control room is unavailable. Other facilities to allow monitoring are provided in the technical support centre.

Suitable fire-fighting equipment and breathing apparatus is provided for the use of operating staff. In the event of the main control room becoming uninhabitable or severely damaged, assured facilities are provided to trip the reactor and isolate the controls so that control can be transferred to the auxiliary shutdown room.

Fire is the only hazard that is considered to have the potential to require the evacuation of the main control room, and in view of the precautions outlined above, this is a very unlikely occurrence.

Communication facilities are provided for on- and off-site communications relating to normal operations, maintenance, site incidents, nuclear emergencies and for general administrative purposes.

2.13. Station Blackout (4.2.3.11)

Simultaneous loss of off-site and on-site AC electrical power (station black-out) is an event of low frequency, due to the provision of reliable off-site connections to the electrical grid by two independent lines, and the on-site four-train essential electrical system supported by four segregated diesel generators.

In the event of station blackout, reactor decay heat removal will be carried out by the Auxiliary Feedwater System (AFWS) using the steam turbine driven feed pumps (see II.2), with steam produced in the steam generators being dumped to atmosphere. The reactor coolant inventory is preserved by the Emergency Charging System, which provides water for the reactor coolant pump seals, and which also has direct steam turbine drive pumps. The inventory of treated water for these systems is sufficient to maintain safe conditions under black-out conditions for at least 24 hours.

The controls necessary for these systems are provided by battery-backed low voltage electrical systems which will continue to be available after the loss of other AC supplies.

2.14. Control of accidents within the design basis (4.2.3.12)

Extensive information is provided to the operator in the Main Control Room under all operating conditions within the design basis. This information includes direct post-fault monitoring of safety functions, limits of operation monitoring to ensure the station remains within safe limits, information on the important parameters during fault conditions, and diagnostic aids. Abnormal developments and transients are normally counted by the inherent reactivity feedbacks and the automatic controls. Where parameters go beyond the safety trip limits, the reactor protection system ensures the reactor is automatically tripped and the Engineered Safety Features are initiated automatically in fault conditions. The design is such that no operator intervention is required for at least 30 minutes. The operator's role in these early stages of the fault is to ensure that systems have responded correctly to the fault conditions, and in the longer term to shut down or start up systems appropriate for maintaining a safe shutdown condition.

The operational documentation includes the Technical Specifications which define the limits which must be observed during operation, and the Emergency Plan and Handbook, which, in the event of a serious fault, ensures the operators have correct guidance on steps to minimise the radiological risk to the public.

2.15. Mitigation and control of severe accidents

The ability of the containment to provide mitigation of the consequences of severe accidents involving core melt has been discussed in Section 2.10, showing that a valuable degree of risk reduction is obtained in these situations.

As far as high pressure core melt sequences leading to direct containment heating are concerned, it is considered that the containment will survive the effects of such sequences. However, as part of the severe accident mitigation procedures, the operator is instructed to depressurise the primary circuit prior to vessel failure using the pilot operated safety relief valves which have very large vent capacity.

The conditions in the containment in severe accidents change and develop quite slowly, giving the operator adequate time to implement accident management procedures which are clearly defined in advance.

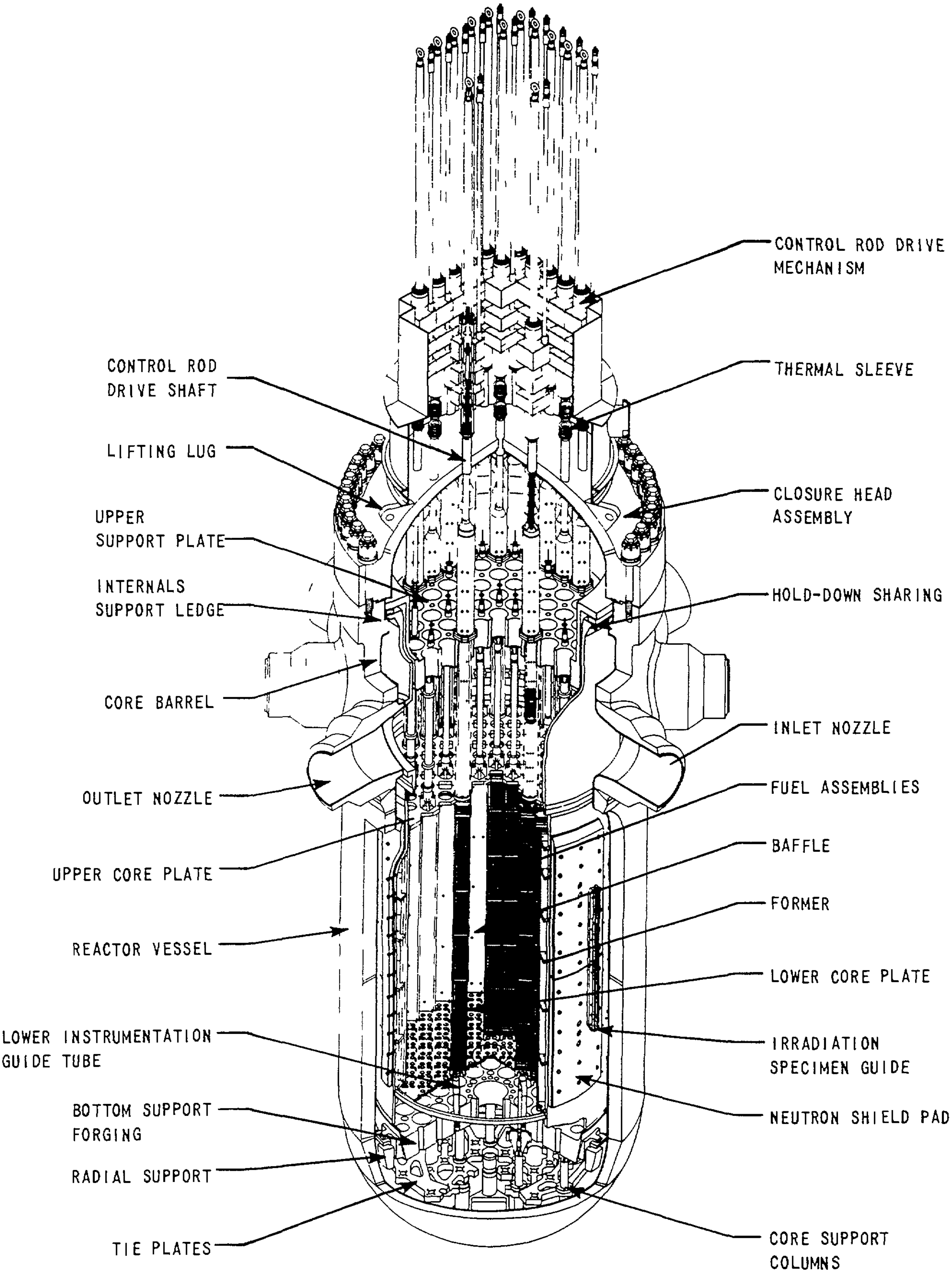


Figure 1 Reactor Pressure Vessel

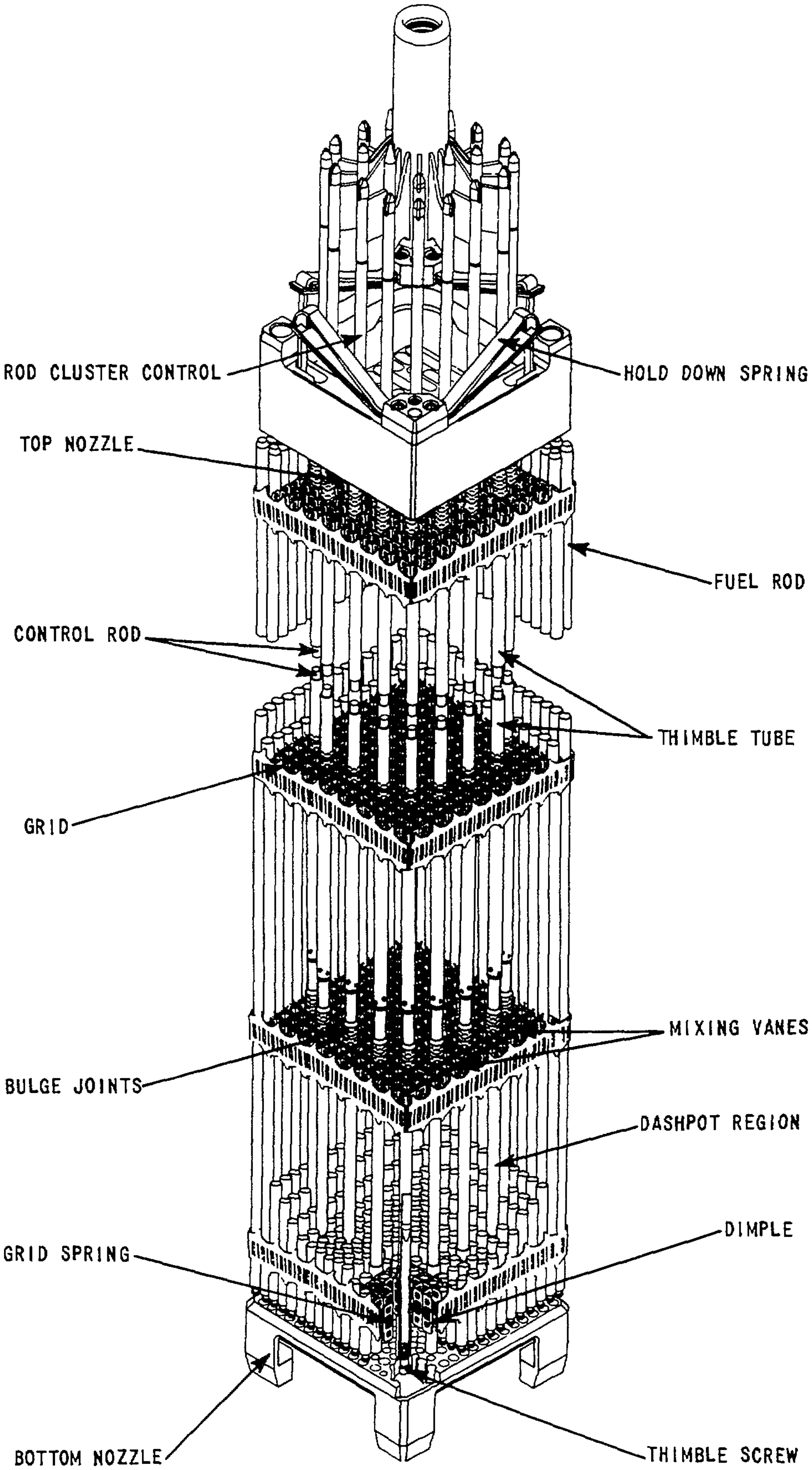


Figure 2 Fuel Assembly

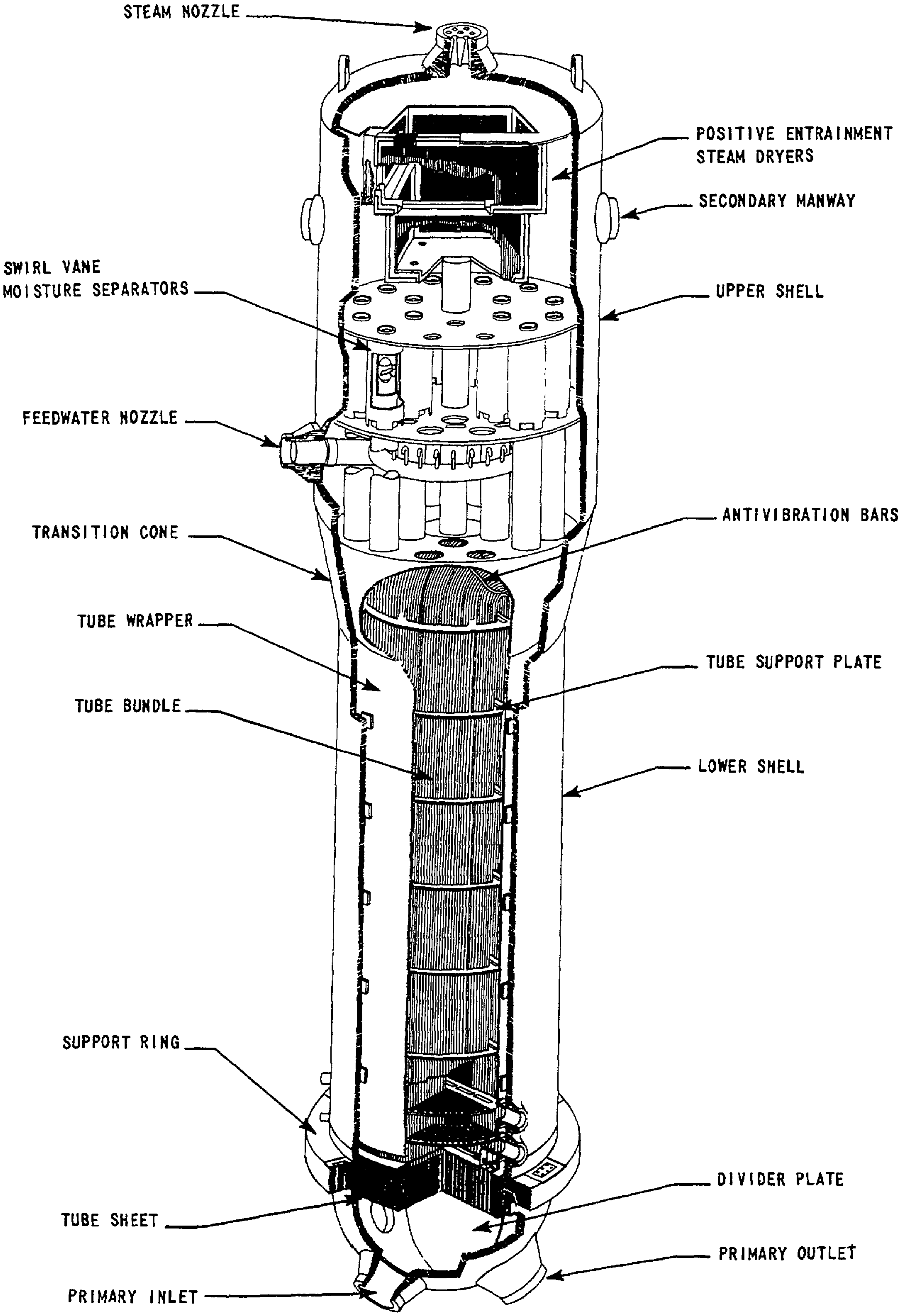
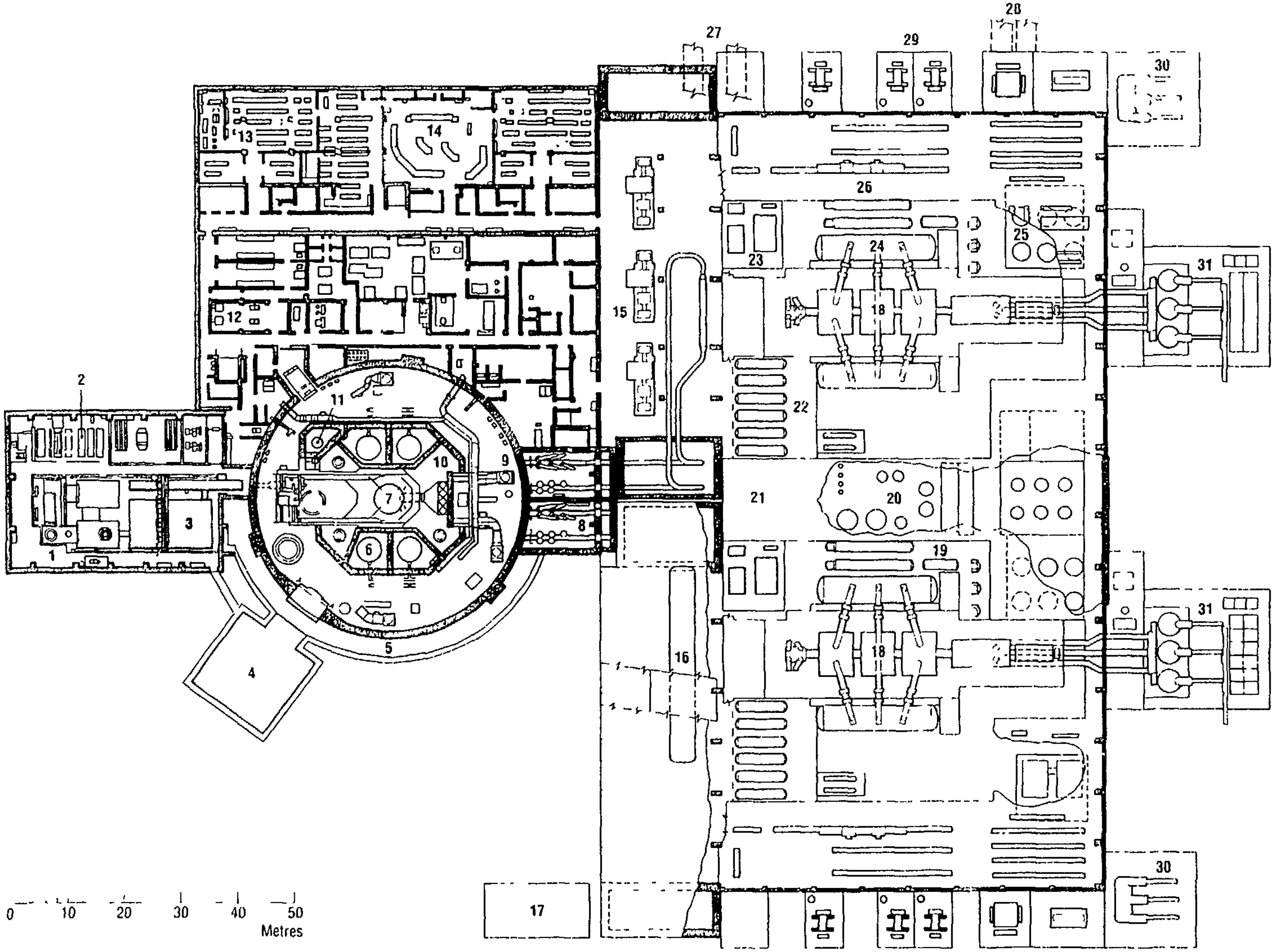


Figure 3 Steam Generator



1	Fuel building
2	New fuel
3	Fuel store
4	Plant access hatch
5	Secondary containment
6	Steam generators (four)
7	Reactor pressure vessel
8	Steam mains
9	Ventilating plant
10	Reactor coolant pumps
11	Pressuriser
12	Auxiliary building
13	Control building
14	Main control room
15	Feed pumps (six)
16	Deaerator
17	Auxiliary boiler house
18	Turbo-generator
19	Low pressure heaters
20	Auxiliary plant
21	Loading bay
22	High pressure heaters
23	Lubricating oil plant
24	Reheaters
25	Polishing plant
26	Switchgear
27	Circulating water outlet
28	Circulating water inlet
29	Transformers
30	Station transformers
31	Generator transformer

Figure 4 Plan of Main Power Block

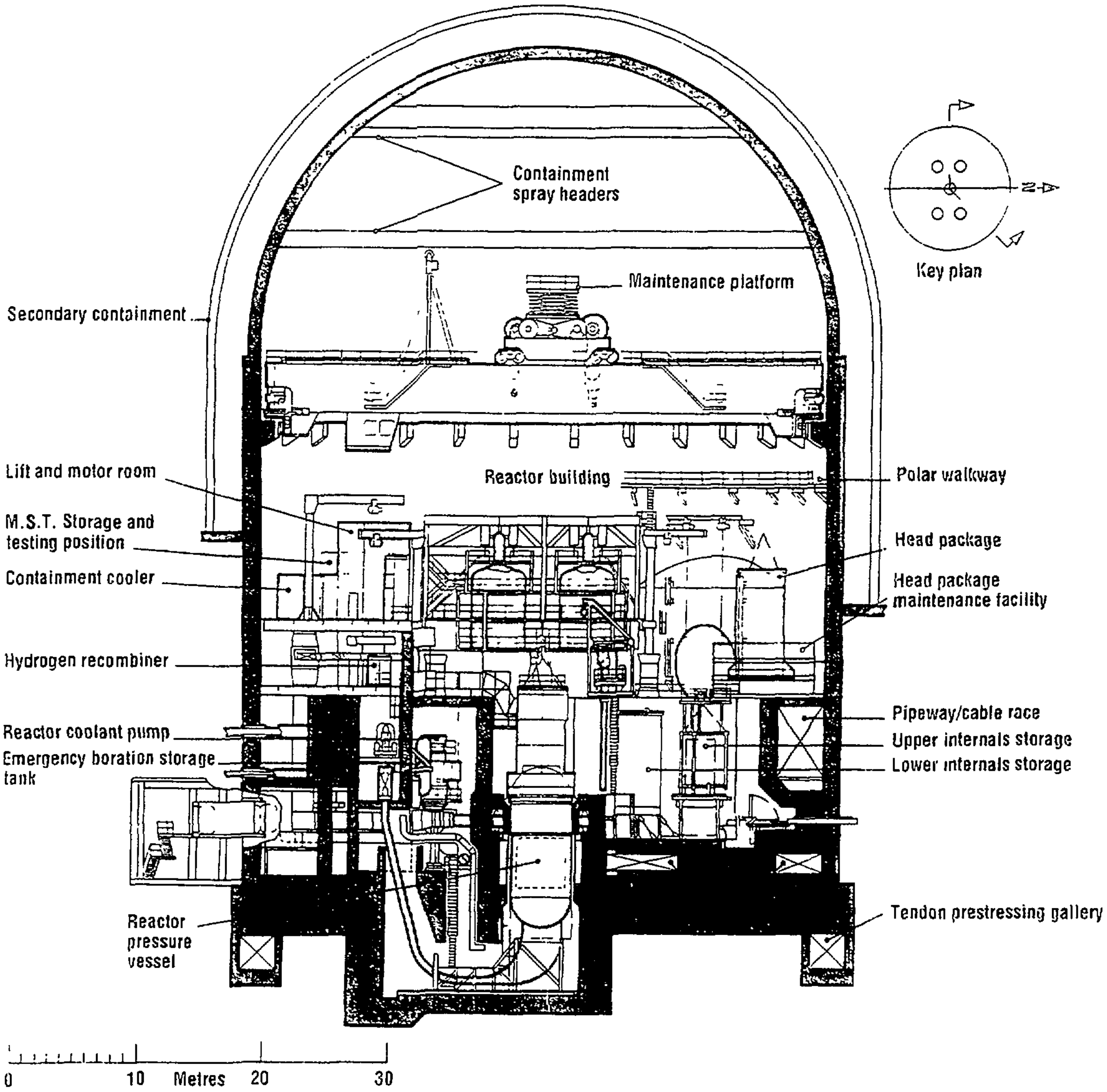


Figure 5 Section through Reactor Building

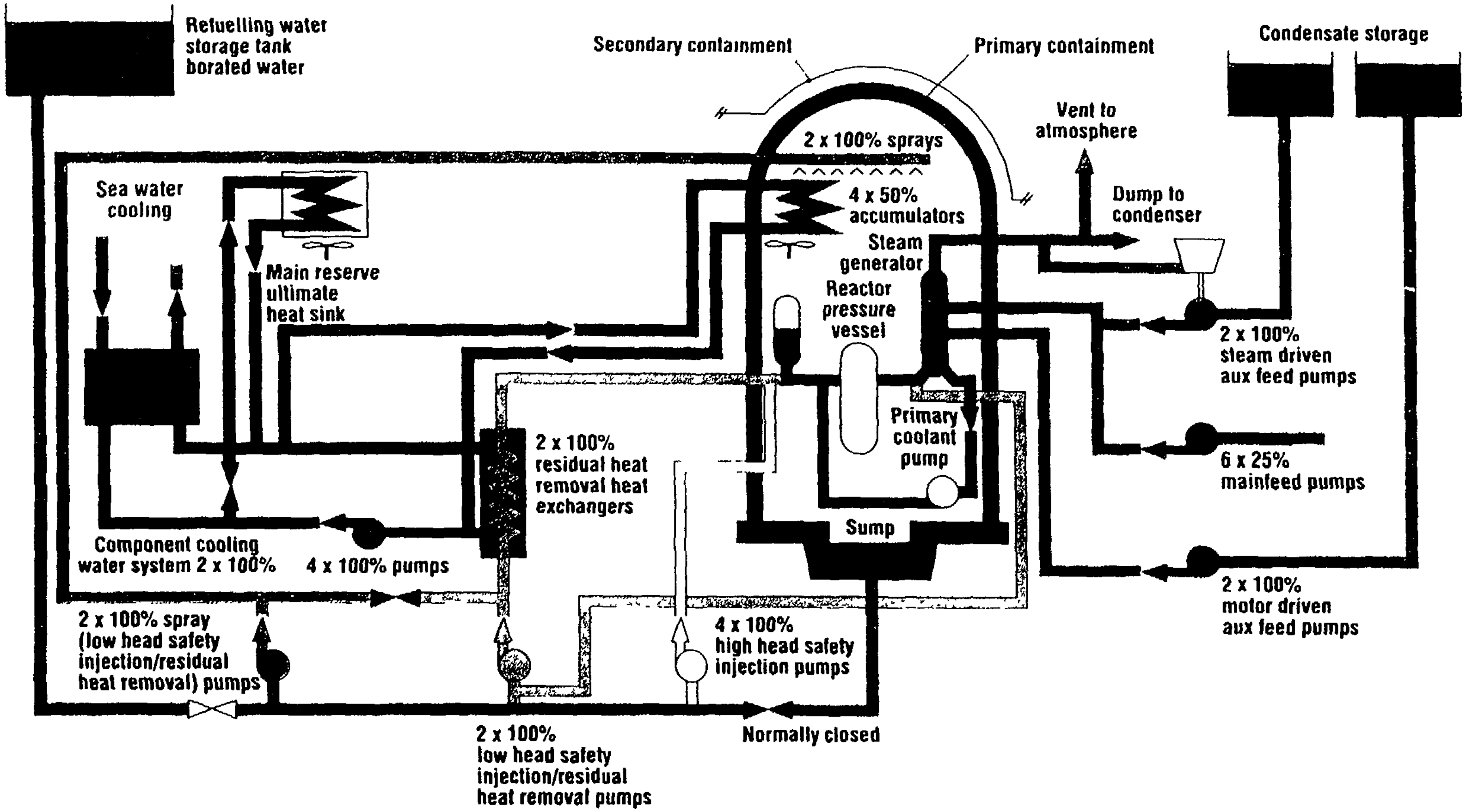

Refuelling water storage tank borated water
Secondary containment
Primary containment
Condensate storage
2 x 100% sprays
Vent to atmosphere
Sea water cooling
4 x 50% accumulators
Dump to condenser
Steam generator
Main reserve ultimate heat sink
Reactor pressure vessel
2 x 100% steam driven aux feed pumps
2 x 100% residual heat removal heat exchangers
Primary coolant pump
6 x 25% mainfeed pumps
Sump
Component cooling water system 2 x 100%
4 x 100% pumps
2 x 100% motor driven aux feed pumps
2 x 100% spray (low head safety injection/residual heat removal) pumps
4 x 100% high head safety injection pumps
2 x 100% low head safety injection/residual heat removal pumps
Normally closed

Figure 6 Engineered Safety Features

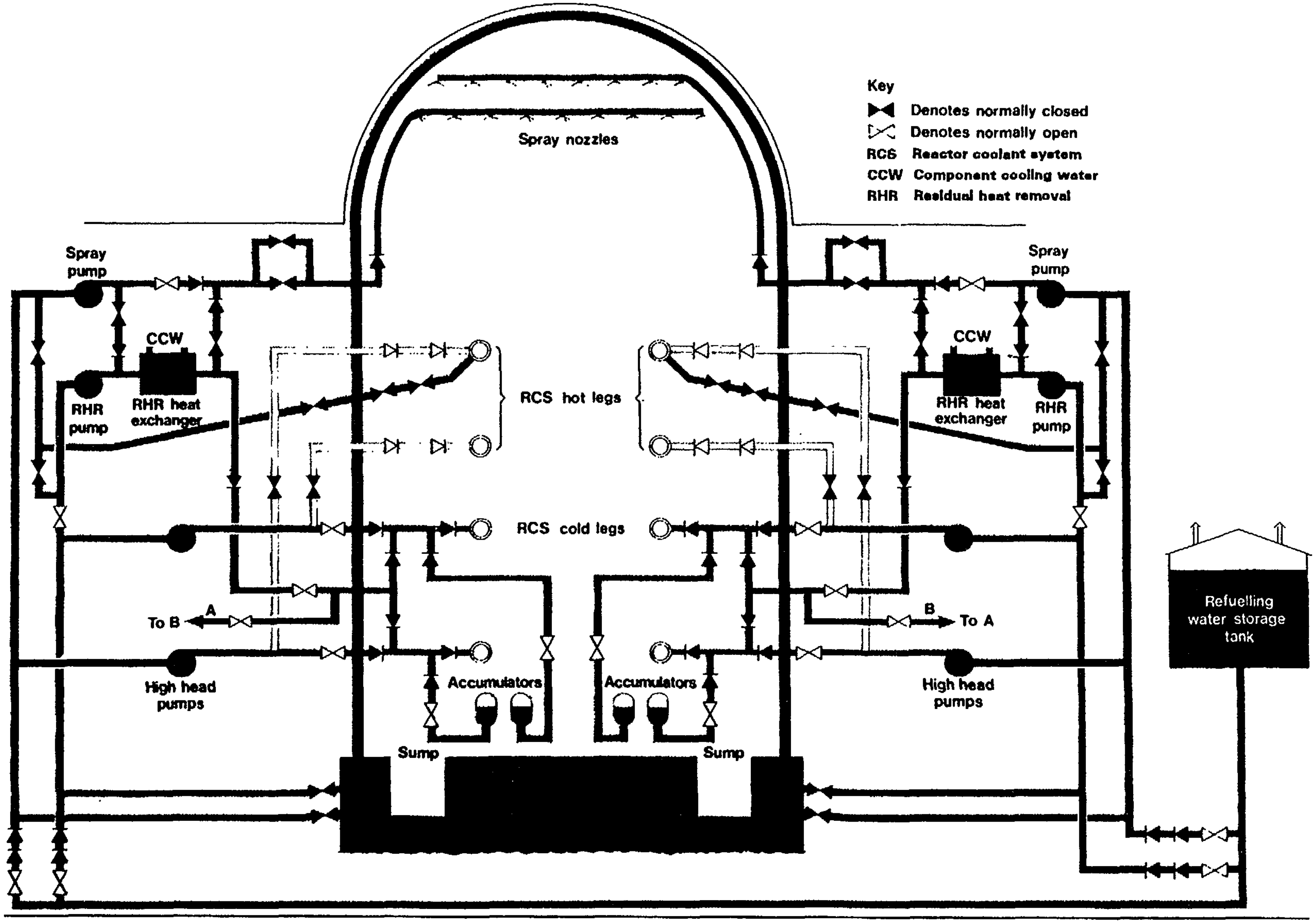


Figure 7 Safety Injection, Residual Heat Removal & Spray System

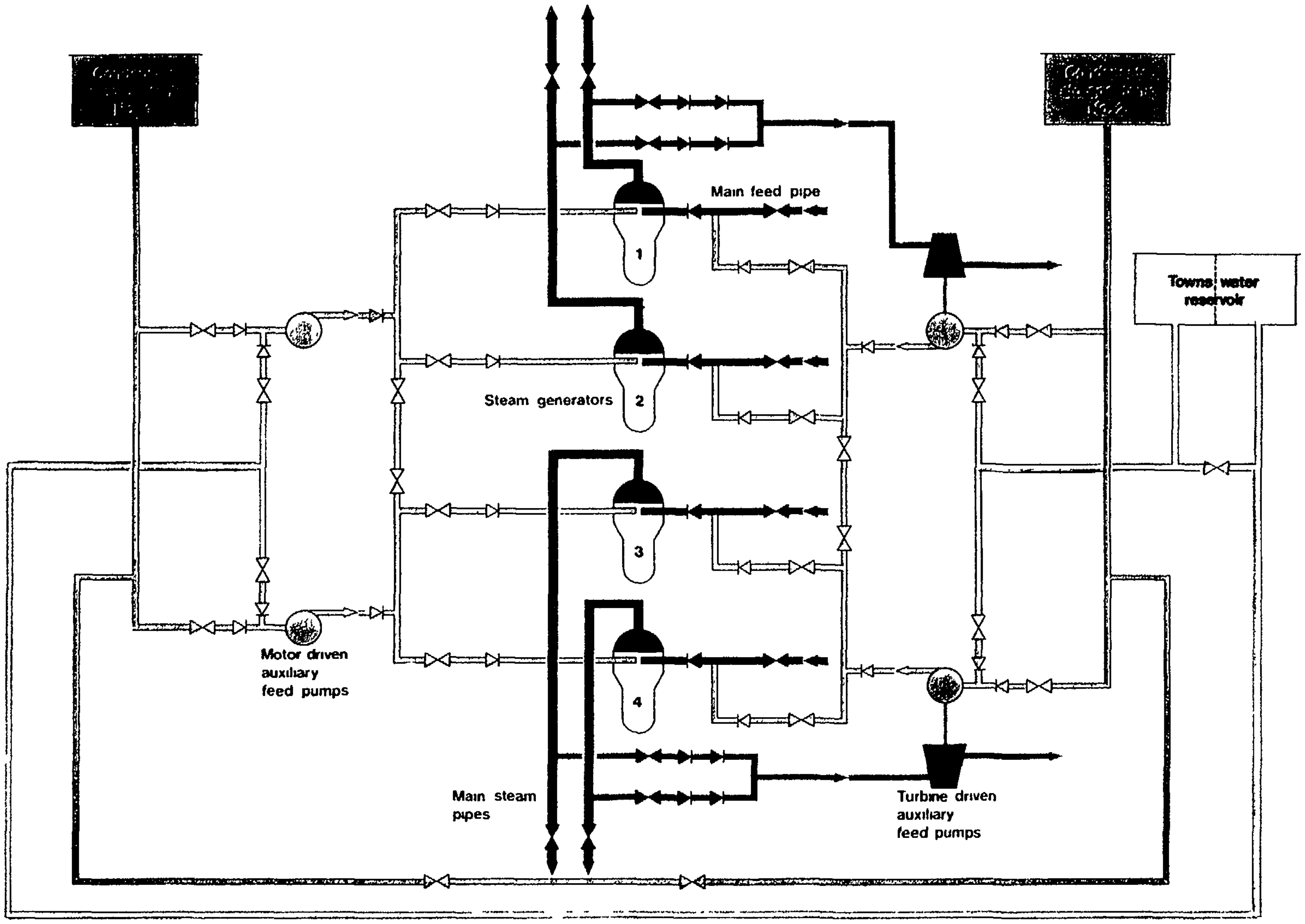


Figure 8 Auxiliary Feedwater System

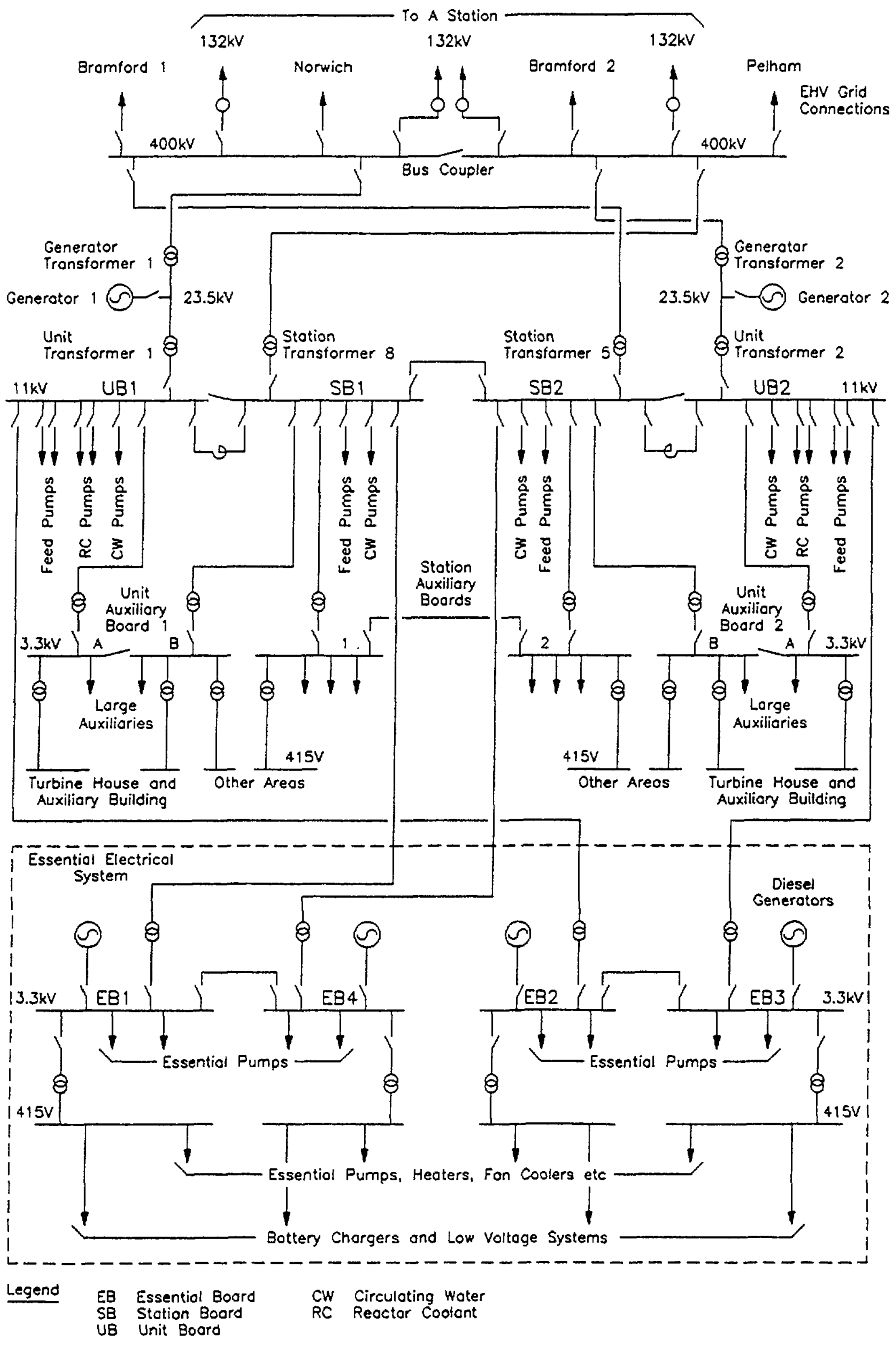


Figure 9. Main & Essential Electrical Systems Diagram

3. EXTENDED DATA LIST

General

Type of reactor	PWR
Number of reactors	1
Number of turbo-generators	2
Area occupied by the station	16.7 hectare

Station output

Rated thermal power of reactor	3411 MW
Gross electrical output	1258 MW
Station internal power consumption	70 MW
Net electrical output	1188 MW

Fuel

Fuel pellets, Material	sintered UO_2
Density	95%
Enriched (feed fuel)	3.1%
Fuel can, Material	Zircaloy 4
Outside diameter	9.5 mm
Thickness	0.57 mm
Fuel assemblies, Basic rod array	17 x 17
Fuel rods per assembly	264
Rod pitch	12.6 mm
Number of guide tubes	
For absorber	24
For instrumentation	1
Number of grids	8

Reactor core

Number of fuel assemblies	193
Active height	3.66 m
Equivalent diameter	3.37 m
Mass of UO_2 in core	101 tonne
Control rod absorber material	Ag-In-Cd
Number of assemblies	53
Absorber rods per assembly	24
Fuel rod heat rating	
Average	17.8 kW/m
Maximum	41.3 kW/m
Moderator	reactor coolant water (H_2O)

Coolant

Operating conditions	
Pressure at vessel inlet	158.3 bar a (15.83 MPa)
Pressure at vessel outlet	155.1 bar a (15.51 MPa)
Temperature vessel inlet	292.4°C
Temperature vessel outlet	323.4°C
Flow rate	19.2 tonne/s
Volume of water in primary circuit	334.5 m^3

Reactor vessel

Overall height	13.59 m
Inside diameter	4.394 m
Total thickness (opposite the core)	220 mm
Material	low alloy steel
Internal cladding	stainless steel
Cladding thickness	7 mm
Inlet nozzle inside diameter	704 mm
Outlet nozzle inside diameter	736 mm
Dry weight	435 tonne

Steam generator

Number	4
Overall height	20.8 m
Upper part diameter	4.51 m
Lower part diameter	3.48 m
Materials	
Secondary side shell	low alloy steel
Tubes	inconel 690
Primary side shell	low alloy steel clad with stainless steel
Tubesheet thickness	631 mm
U-tubes, Number	5626
Outside diameter	17.46 mm
Thickness	1.03 mm
Total heat transfer area	5110 m^2
Dry weight	377 tonne
Reactor coolant side	
Inlet temperature	326.4°C
Outlet temperature	293.8°C
Flow rate	4.8 tonne/s
Secondary steam side	
Feedwater temperature	227°C
Steam temperature	285°C
Steam pressure	69 bar a (6.9 MPa)
Steam flow rate	477 kg/s
Steam condition	0.25% wetness

Reactor coolant pump

Number	4
Speed (synchronous)	1500 rpm
Developed head	89.3 m
Flow rate	6.45 m^3/s
Pump bowl material	stainless steel
Motor rating	6 MW
Dry weight	103 tonne

Pressuriser

Number	1
Overall height	16.1 m
Inside diameter	2.13 m
Volumes, Total	51.0 m^3
Water at full power	30.6 m^3
Heaters, Number	78
Total heater power	1.8 MW
Pilot-operated relief valves	
Number	3 pairs
Capacity (sat steam at 172 bar) per pair	34 kg/s
Safety relief valves	
Number	2
Opening pressure	172.4 bar a (17.24 MPa)
Capacity (at that pressure) per valve	53 kg/s
Pressuriser relief tank	
Total volume	51 m^3
Normal liquid volume	38 m^3
Design pressure	7.9 bar a (0.79 MPa)
Rupture disc burst point	6.3 bar a (0.63 MPa)

Reactor coolant pipes

Inside diameters	
Hot leg	739 mm
Intermediate leg	790 mm
Cold leg	699 mm
Pressurizer surge line	284 mm
Material	stainless steel

Accumulators

Number	4 x 50%
Total volume per accumulator	57.3 m^3
Water volume per accumulator	36.1 m^3
Nitrogen overpressure	45.8 bar g (4.68 MPa)
Material	carbon steel clad with stainless steel

Auxiliary and safeguard system pumps CVC charging pumps

Number	2 x 100%
Design flow	33.4 m^3/h
Design head	1782 m

Emergency charging pumps

Number steam driven	2 x 100%
Design flow (seal injection mode)	9.08 m^3/h
Design head	172.4 bar

Residual heat removal pumps/low head safety injection pumps

Number	2 x 100%
Design flow	568 m^3/h
Design head	160 m

Spray pumps

Number	4 x 100%
Design flow	795 m^3/h
Design head	145 m

Safety injection pumps

Number	4 x 100%
Design flow	227 m^3/h
Design head	964 m
Maximum delivery head	1250 m

Component cooling water pumps

Number	4 x 100%
Design flow	2846 m^3/h
Design head	36 m

Auxiliary feedwater pumps

Number - motor driven	2 x 100%
Design flow	135 m^3/h
Design head	1162 m
Number - turbine driven	2 x 100%
Design flow	189 m^3/h
Design head	1019 m

Turbine conditions

Speed	3000 rpm
Pressure at inlet	66.6 bar a (6.66 MPa)
Temperature at inlet	282°C
Flow rate at inlet	955 kg/s

Condensate extraction pumps

Number per turbine	3 x 50%

Main feedwater pumps

Number per turbine	3 x 50%
Drive	induction motor
Flow rate per pump	0.548 m^3/s
Developed head	935 m
Speed	variable
Temperature	156°C

Circulating water pumps

Number per turbo-generator	2 x 50%
Flow rate per pump	12 m^3/s
Developed head	9 m
Power of the motor	1.4 MW

Containment

Primary	
Type	prestressed concrete with carbon steel liner
Inside diameter	45.7 m
Inside height	64 m
Wall thickness	1.3 m
Liner thickness	6 mm
Design pressure	3.45 bar g (0.445 MPa)
Secondary	
Type	reinforced concrete

Refuelling water storage tank

Water storage volume	1775 m^3
Boric acid concentration	2000 ppm
Material	stainless steel

TECHNICAL INFORMATION ON DESIGN FEATURES OF SIEMENS KONVOI PWR

J. CZECH, A. FEIGEL, P.-J. MEYER
Siemens AG, KWU,
Erlangen

A. KREMAYR
Bayernwerk AG,
Munich

Germany

Abstract

The paper describes the Konvoi PWR plant design of Siemens, Germany. The paper consists of three parts: - a general description; - a description of how the plant compares with the safety principles of INSAG-3 for 15 selected design areas; and - an extended data list. The general description outlines the main elements of the safety philosophy, general plant characteristics, and risk reduction strategy. The second part discusses plant performance in the areas of: - plant process control systems; - automatic safety systems; - protection against power transient accidents; - reactor core integrity; - automatic shutdown systems; - normal heat removal; - emergency heat removal; - reactor coolant system integrity; - confinement of radioactive material; - protection of confinement structure; - monitoring of plant safety status; - preservation of control capability; - station blackout; - control of accidents within the design basis; and - mitigation and control of severe accidents. The third part, finally, presents data related to the power plant as a whole, data on reactor core and fuel, on the reactor coolant system, the reactor pressure vessel, coolant pumps, steam generators and pressurizer, and on the containment.

1. GENERAL DESCRIPTION

1.1. Introduction

In Germany, 21 LWRs with a total generation capacity of 22,365 MW are currently operating, among them there are 13 PWRs with 15,158 MW and 8 BWRs with 7,207 MW. The main reactor type preferably used for energy production is the PWR. The last series of PWRs built in Germany is the standardized type of Konvoi Concept. This generation of PWR in Germany could already be called "advanced" technology compared to development targets specified for the next generation of PWR plants in other countries. However, there is always space being left for further improvements in the technical field. For Konvoi, in the frame of backfitting measures further improvements with respect to severe accidents were adapted.

The first part of this paper outlines the Konvoi technology as having been built and operated with an outstanding availability and minimized radiation exposure. In the second part of this paper the description is provided, how the key features in 15 design areas according to INSAG-3 are fulfilled. The third part contains the extended data list.

1.2. The main elements of the safety philosophy

Further improvements compared to previous PWR, are principal characteristics of Konvoi-PWR based on experience from plant operational feedback and insights gained by PSA studies. Therefore, the design incorporates a balanced measure of design margin, accident prevention, accident control and additional measures for residual risk reduction. The Konvoi design is in compliance with national codes and standards in Germany.

As a result, the probability of core damage for the Konvoi design has been reduced by about one order of magnitude compared to previous plants. In the residual risk reduction area, not only rare external events but also events which could lead to core melt as a result of hypothetical beyond design basis accidents involving multiple system failures as well as mitigative measures in case of core melt situations are dealt with (preventive and mitigative emergency procedures).

1.2.1. Defense-in-depth concept

A defense-in-depth safety concept with several safety levels is applied in accordance with Criterion 1.1 of the German "Safety Criteria for Nuclear Power Plants" in order to fulfill the safety objectives:

- Shutdown and long-term subcriticality of the reactor
- Residual heat removal
- Minimization of radioactive releases

This concept consists of a balanced combination of priority actions to prevent malfunctions and accidents and actions to contain and control those accidents which are nevertheless postulated as the design basis of the plant. It also includes actions to mitigate the consequences of beyond-design-basis events, occurrence of which can be practically ruled out. This safety concept is described in the following.

First Safety Principle: Accident Prevention

At the normal operation level (1st safety level), high availability is assured by quality of plant design and manufacture and diligence in the conduct of plant operations. In terms of safety, this is important in that high availability means few malfunctions and accidents.

The first safety level thus consists in safety-enhancing design, fabrication and plant operation principles, for instance:

- Sufficient safety allowances in the design of all plant items and systems
- Careful selection of materials backed up by extensive materials testing
- Comprehensive quality assurance in manufacture, construction and operation
- Independent verification of the quality attained
- In-service inspections to monitor quality after service loading
- Ease of maintenance of plant items and systems, hence low radiation exposure of personnel
- Reliable monitoring of operating conditions

- Recording, analysis and feedback of operating experience as the basis for enhancing safety
- Extensive training of operating personnel.

General engineering experience shows that, in spite of application of these principles, malfunctioning of plant items or systems which leads to upset operating conditions during the service life of a plant cannot be completely ruled out. Typical examples are mechanical component failures such as failure of a pump in the reactor coolant system or in the water/steam cycle. Upset operating conditions are kept within allowable design limits for normal operation. Limit values and their monitoring control are used to prevent accidents resulting from upset operating conditions. Once the cause of the malfunction has been eliminated, operation of the plant may be continued without restriction. Such precautions at the second safety level are, for instance:

- Inherent safety of the reactor core; this means that the reactor returns of its own accord to stable power, temperature and pressure equilibrium conditions even if control features fail as a result of minor operational malfunctions.

This is achieved by means of a core physics design with negative temperature coefficients of reactivity. In addition, the following is emphasized:

- Status signals and alarms are transmitted to the control room and recorded to keep the operators informed so that they can take manual actions.
- Multiple protective and limiting controls work actively to prevent operational malfunctions from escalating into accidents. These controls are provided in addition to the control systems already active in normal operation and serve to initiate corrective actions on the final control elements, e. g. to reduce reactor power, before unacceptable operating conditions are attained. These actions are backed up by the inherent safety features of the reactor core.

The safety I&C system comprises the functions of limiting controls and reactor protection. The limiting controls respond selectively and as appropriate to the specific operational malfunction; if they are unable to terminate the operating transient in time, the reactor protection response limits are violated. Examples of such limiting functions are the reactor protection limitation and the coolant inventory and pressure limitation function for the reactor coolant system.

None of the events postulated to occur at the 1st safety level (normal operation) and 2nd safety level (operational malfunctions) causes the dose limits established in Section 45 of the German Radiological Protection Ordinance to be violated.

Second Safety Principle: Accident Control

At the 3rd safety level, to protect against damage, Konvoi is also designed to withstand postulated accident conditions which, given the spectrum of measures already taken to prevent accidents, to the best of human knowledge need not be anticipated to occur at all (design basis accidents). The design basis accidents are defined such that each is representative of a group of similar events, i. e. that they yield the load conditions representative of that group of events for the purposes of plant design. As part of the licensing procedure, it is demonstrated that these design basis accidents can be contained and controlled without the dose limits of Section 28 Para. 3 of the German Radiological Protection Ordinance being violated.

The events which the plant must be designed to control are postulated in accordance with the German "Guidelines for the Review of the Design for Accidents of Pressurized Water Reactor Nuclear Power Plants pursuant to Section 28 Para. 3 of the German Radiological Protection Ordinance - Accident Guidelines". The spectrum of design basis accidents includes both internal events, e. g., breaks and leaks in a reactor coolant line, and external events, such as earthquake, and is divided into four categories:

RA: The radiologically representative accidents must be calculated regarding their radiological impacts.

AS: These accidents are analyzed for the purpose of designing engineered safety features or counteractions.

SI: The analysis of these accidents is used for the purpose of designing components or structural items for stability or integrity.

VO: An accident analysis is not necessary if the precautionary measures specified in the Accident Guidelines are demonstrated to have been taken. The accident concerned is prevented or controlled by these precautionary measures.

The categories AS, SI and VO are also taken into account in the accident control philosophy and the residual risk reduction philosophy.

Firstly, the engineered safety features provided to withstand these accidents consist of passive systems. These are facilities which need no command signals or power input in order to fulfill their safety functions but act simply by their presence; examples are the numerous concrete and steel barriers.

Secondly, active safety facilities are also provided, for example the safety injection pumps, which are controlled and put into action by the safety I&C system when and as necessary.

Third Safety Principle: Residual Risk Reduction

Further to the actions taken to prevent and to contain accidents, actions are taken at the 4th safety level to mitigate the impact of events which, because of the low risk they represent, are not classified as design basis accidents. This group of events includes:

- Extremely infrequent external events such as aircraft crash and collision of transport vehicles with buildings;
- Internal events which could end in core meltdown as a result of hypothetical beyond design basis accidents involving multiple system failures ("residual risk events").

The actions taken to combat these extremely infrequent events are ad hoc actions specially tailored to the essential aspects of the specific events in consideration of achieving a reasonable balance between the engineering effort involved and its achievable risk reduction.

Precautions against extremely infrequent external events essentially take the form of structural protective features.

The aim of the counteractions taken against internal residual risks events is to mobilize for the purpose of risks minimization any safety reserves existing in the plant above and beyond the design basis pursuant to Section 28 Para. 3 of the German Radiological Protection Ordinance. The approach applied in engineered safety features results in considerable oversizing components and systems and the provision of redundant systems on the basis of the single failure criterion. Considered realistically, and taking into account the safety reserves of the components, these systems actually are significantly more effective, than postulated, and this would enable them to be used in a versatile fashion to control internal events at the residual risk probability level.

This applies especially to in-plant emergency procedures. Safety studies, reactor safety research and risk studies have systematically investigated the question as to what actions can be taken to avert, with high probability, serious core degradation and severe environmental impacts arising out of internal events which, if allowed to take their course uncontrolled as a result of hypothetical beyond design basis system failures, could lead to core meltdown.

1.2.2. Engineered safety features

The fundamental principle behind the design of the engineered safety features is:

- on the one hand to make faults and operational malfunctions as improbable as possible by means of procedures such as safety margins in design, use of proven and type-tested components, and in-service inspections at regular intervals.
- While on the other hand systematically postulating faults and malfunctions within the terms of reference of the single failure concept (as expounded in the Interpretations of the Safety Criteria for Nuclear Power Plants published by the Federal Ministry for the Interior on 10.05.1984) so as to ensure that the design of the engineered safety features permits such failures, if they should occur, to be reliably contained and that the proper functioning of the engineered safety features is assured to the necessary extent.

There follows a review of the criteria and design principles applied in the implementation of this fundamental principle and thus in the design of a fault-tolerant safety technology.

1.2.2.1. Passive engineered safety features

The Barrier Concept

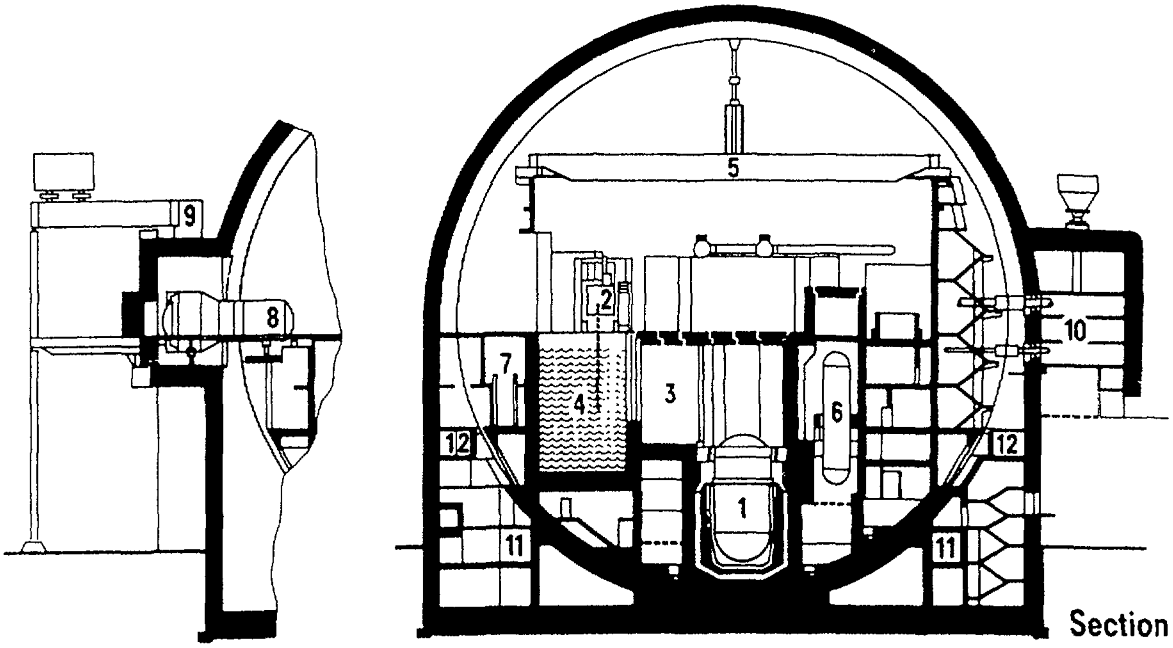
Reliable confinement of the radioactivity produced in nuclear fission is achieved by series of barriers which provide defense-in-depth against escape of radioactive materials:

- the fuel matrix
- cladding tubes
- reactor coolant pressure boundary
- containment

The gas-tight, spherical steel containment is of special importance to the protection of the environment. Since it is the final barrier, it must remain fully operable should all other barriers fail, i.e. it is designed to withstand the most severe loss-of-coolant accident in the course of which the contents of the entire reactor coolant system are assumed to evaporate into the containment.

The containment in turn is protected by a reinforced concrete shell to protect the reactor from external impacts, see figure 1. The concrete shell is thick enough to withstand, for instance, the impact of a military aircraft flying at high speed. In the various compartments of the reactor building, the ventilation systems maintain a negative pressure (relative to atmospheric air pressure) which becomes stronger towards the center of the building. Thus, only in-leakages can occur, and no radioactivity can escape uncontrolled into the environment. The exhaust air can be passed through high-efficiency filter systems before being discharged to the vent stack. The integrity of the radioactivity retaining barriers is checked by continuous measurement of radioactivity levels in the various process cycles and compartments.

Further to the barriers provided to retain radioactivity and to protect the reactor against external impacts, there are also barriers that serve to shield line-of-sight radiation from the reactor core. These take the form of thick concrete walls. The concrete shield around the reactor pressure vessel, for instance, is about 2 meters thick. The 25 cm thick steel shell of the reactor pressure vessel itself is also an effective radiation shield. The line-of-sight radiation leaving the nuclear power plant during normal operation is so low that it cannot be measured against the natural radiation background outside.



1 Reactor pressure vessel
2 Refuelling machine
3 Lay down position
for core internals
4 Fuel pool

5 Reactor building crane
6 Pressurizer
7 New fuel store
8 Equipment lock

9 Gantry
10 Main steam and feedwater valve room
11 Pipe duct
12 Cable duct

Fig. 1: **PWR 1300 MW Reactor Building**

1.2.2.2. Active engineered safety features

The effectiveness of the fission product barriers and radiation barriers must be maintained not only in normal operation and under upset conditions but also in the event of postulated accidents to such an extent that unacceptable releases of radioactivity into the environment is prevented. To ensure their effectiveness, the barriers are designed to withstand the loads occurring during such accidents and are protected by active engineered safety features.

The active engineered safety features are designed especially to be able to control such situations, that is specifically, to shut down the reactor safely from all operating conditions and to ensure the removal of the decay heat from the reactor core.

To ensure the high reliability required of the safety features, several system design principles are applied:

- redundancy
- diversity
- physical separation of safety system trains and separation of safety systems from operational tasks
- fail-safe principle

Redundancy

The redundancy principle is applied to cope with single failures. Single failure is postulated in addition in the demand mode independent from the initiating event and not as a consequence of the accident. Single failure is applied to passive and active components.

Single failure is required in Germany also during repair or maintenance. Only for very rare events (e.g. airplane crash) deviations are allowed. The consequence of postulating single failure and repair results in a n+2 redundancy of engineered safety features with consequential train separation including I&C, power supply and auxiliary systems.

Diversity

The diversity principle is applied in special sectors of the reactor protection system to prevent multiple faults occurring at the same time due to the same cause, e. g. design error or manufacturing defect. Diversity denotes variety. Hence, different physical principles and/or equipment designs which cannot all become ineffective or fail at the same time for the same reason are used to fulfill a given safety function. Thus, for example, initiation of reactor trip in response to accident conditions is always based on evaluation of several diverse criteria. For instance, a rise in reactor power, which first makes itself noticed in a rise of the neutron flux, will always also be accompanied by a rise in coolant temperature and, because of thermal expansion of the coolant, by a rise in the water level in the reactor coolant system. In this case, three mutually diverse criteria can be formulated for reactor trip.

Physical separation and structural protection

To prevent disturbances from spreading from one redundant subsystem (train) to another, the trains of the same system are physically separated (Fig. 2). Where single systems or components require protection or where physical separation of redundant subsystems (trains) is not possible or reasonable, suitable structural protection is provided. Examples are the physical separation of cooling water lines to cope with aircraft crash, or the protection of the non-redundant containment, which is essential to radioactivity retention, by designing the reactor building to withstand aircraft crash.

A further instance is the design of important buildings and systems to withstand earthquake.

Fail-safe principle

In certain cases, application of the fail-safe principle affords added protection against all accident mechanisms discussed up to now and against the consequences of loss of auxiliary power, e. g. loss of power supply to the engineered safety features. Fail-safe denotes reversion to a safe condition in the event of a malfunction, i. e., that safety features are designed to initiate a safe action in the event of a malfunction in the safety feature itself or upon loss of its power supply. An example of a fail-safe safety action is dropping of the control assemblies into the core under their own weight to trip the reactor in the event of loss of power supply.

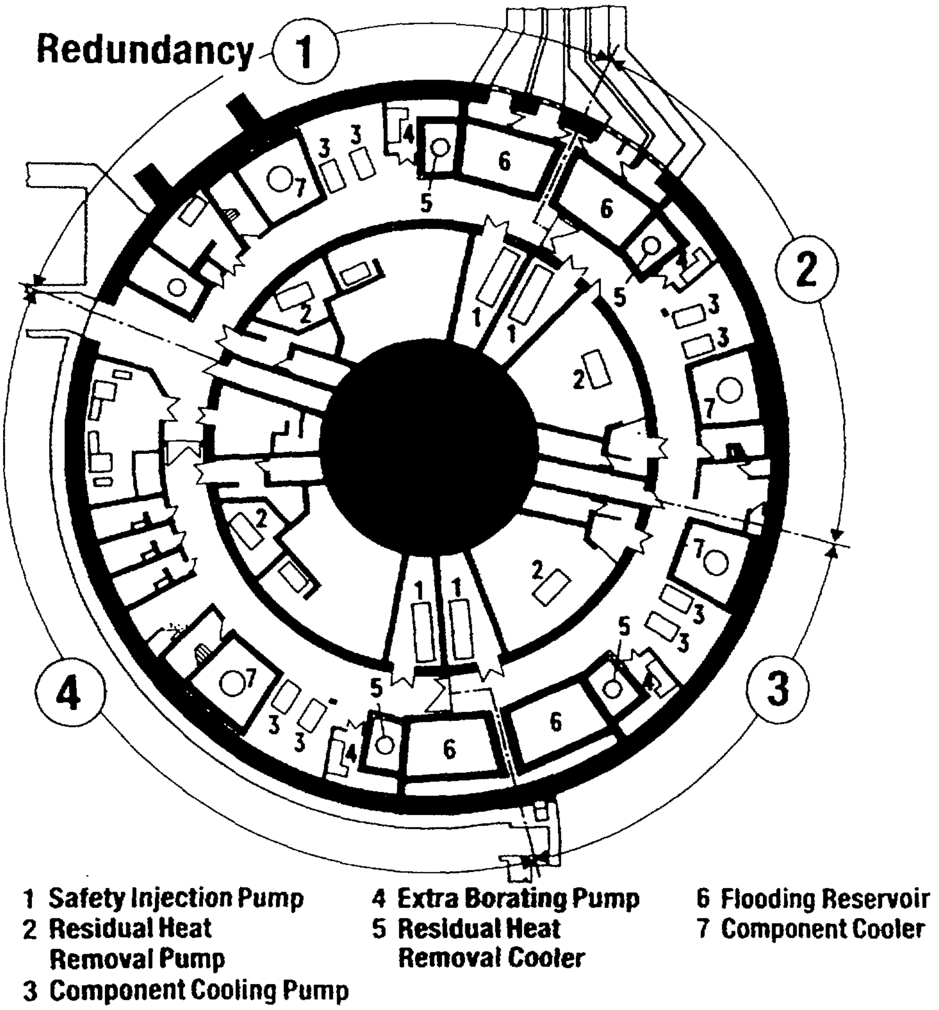


Fig. 2: **Arrangement of the Components Important to Safety Inside of the Reactor Building**

Automation

When rapid transients are involved, it would be unreasonable to rely solely on the attentiveness of the operating crew for detecting malfunctions and on their ability to take the right decision instantly to initiate counteractions. The possibility of errors of analysis or judgement, especially in the first minutes following accident initiation, would be too great. For this reason, no manual actions are required to control an accident in the first 30 minutes after its initiation. The accident control actions taken by the safety I&C are fully automated and override any manual actions by the operating crew.

In addition to the plant concept to cope with rare events the design is such to stabilize automatically the plant for 10 h without human intervention (e. g. loss of main control room in case of airplane crash)

1.3. General plant characteristics

The Konvoi design characteristics imply the entire plant: nuclear island, turbine hall and balance of plant.

The Nuclear Steam Supply System (NSSS) consists of a PWR with four primary coolant loops, a pressurizer connected to one of the loops, 4 steam generators, four reactor coolant pumps (RCPs) and the auxiliary and safety systems directly related to the NSSS (Fig. 3). The NSSS generates approximately 3,782 MWt producing steam at 63.5 bar (6.35 MPa)

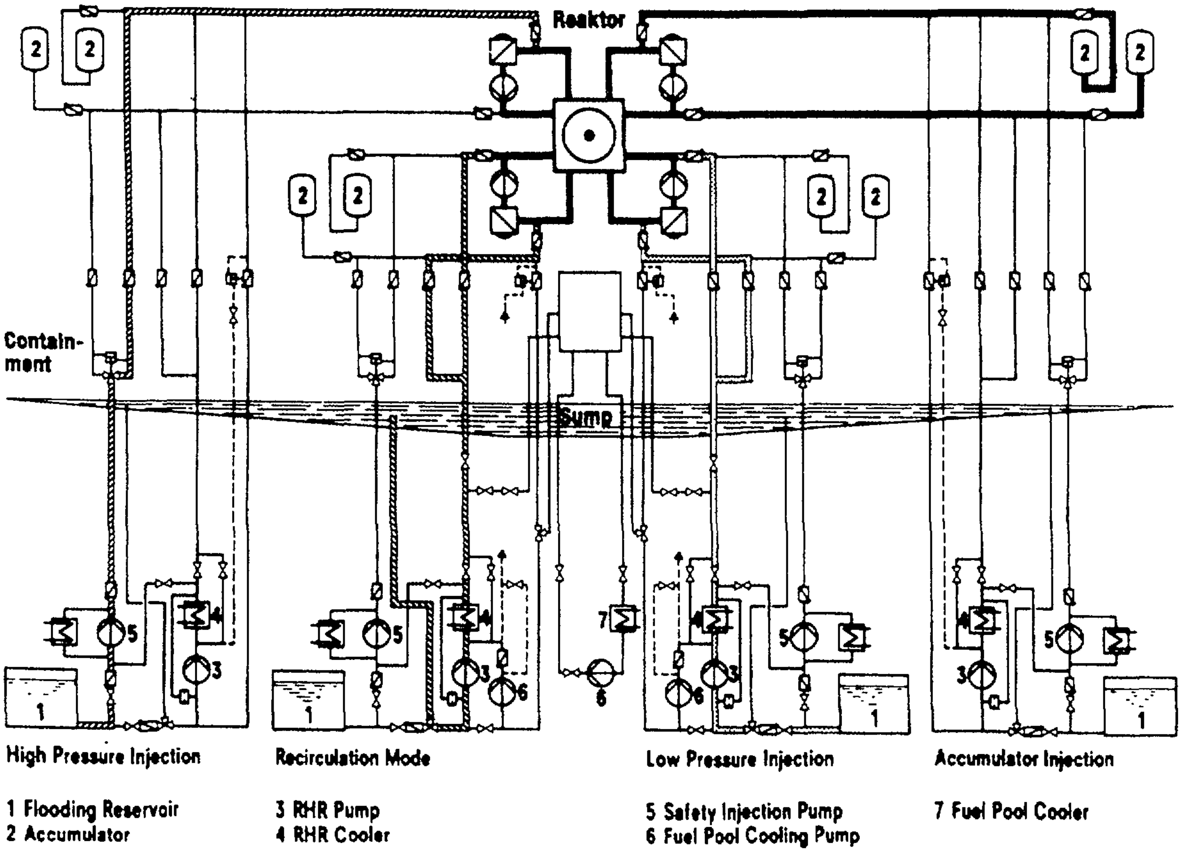


Fig. 3: PWR 1300 MW - Emergency Cooling and RHR-System

at steam generator outlet. The turbine generator provides a net power of approximately 1287 MWe. Full load rejection is accepted without reactor or turbine trip. The turbine plant is completely automatic and is supervised from the control room.

The summary of main safety and operational features is given in table 1.

TABLE 1

Safety goal	Safety function	Systems performing safety functions
Reactivity control	Shutdown	control rods
	Longterm subcriticality	volume control system extra borating system ECC-system
Reactor coolant inventory	Core covering	HH-safety injection LH-safety injection accumulator
	Minimization of leakages	extra borating spray
Primary to secondary side heat transfer	Heat transfer	forced flow with main coolant pumps natural circulation
Primary side pressurizing	Pressurizer overpressure protection	pressurizer spraying pressurizer relief valve pressurizer safety valves
Secondary side heat removal	SG feed	main feedwater pumps start-up and shutdown pump emergency feedwater pumps
	SG overpressure protection	main steam relief valve main steam safety station
	SG steam release	main steam bypass station main steam relief valve
	Limitation of steam release	secondary side isolation
	SG overfeed protection	main feedwater valve system
Primary side heat removal	heat removal from RCS/fuel pool	residual heat removal system component cooling system secured service water system
Limitation of activity release	from containment	containment isolation containment isolation for ventilation
	from annulus	annulus air extraction system
	from steam generator	main steam isolation valve main steam relief isolation valve steam generator blowdown system

1.4. Risk reduction

Besides of rare external events like airplane crash and explosion pressure wave, which have to be analyzed according to the third safety principle of risk reduction in this 4th safety level and for which the plant is designed events which could result in core melting due to complete failure of highly redundant engineered safety features are coped with by preventive emergency procedures.

In addition, if carrying out the preventive emergency procedures fails to avert ongoing core degradation and RPV-meltthrough, damage-mitigating emergency procedures are carried out with the objective of at least maintaining the integrity of the previously isolated containment and to permit only controlled and filtered radioactive releases from it.

Preventive Emergency Procedures

Accidents which could result in core melting are inconceivable except under circumstances in which redundant engineered safety features such as residual heat removal system suffer multiple failure. Although such multiple failures are extremely improbable, preventive emergency procedures to recover residual heat removal after postulated multiple failures of system are provided for. Measures to restore steam generator feed by secondary side bleed and feed take priority. These are backed up by emergency procedures for direct heat removal from the reactor coolant system by opening pressurizer valves (RCS bleed and feed). Prioritization of secondary system bleed and feed is preferable from the point of view of erroneous actuation, and RCS bleed and feed need only be performed as the last resort.

Mitigating Emergency Procedures

If this prerequisite is fulfilled, adequate time is available for further emergency procedures to be carried out in order to avert conceivable late failure of the containment in the further course of the accident as a result of the mechanism:

- formation and explosion of hydrogen in the containment, or
- long-term pressure buildup

Therefore, special measures are applied for hydrogen reduction by including deflagration at an early stage and low hydrogen concentrations. This can be ensured by numerous igniters installed in the various compartment complexes of the containment and recombiners. The so-called Dual Concept is under investigation by the Safety Authorities in Germany.

Assuming that it has been possible to avert early failure of the containment by carrying out the emergency procedures described above, a long-term pressure buildup in the containment is to be expected in the further course of a core melt accident as a result of the mass and energy input. The test pressure of the containment is reached after several days. In order to prevent uncontrolled containment failure by overpressure, a system for filtered venting to the vent stack is provided.

The venting system is designed to restrict the containment to test pressure without water needing to be injected into the sump and combined with water injection into the sump, to reduce the containment to half the test pressure within two days provided that venting is initiated every time test pressure is approached.

The probabilistic risk assessment performed for the Konvoi plant design indicates a significant improvement in the total core damage frequency as a result of incorporating the above stated features. The total core damage frequency for the Konvoi is below 10^{-6}/year taking into account preventive emergency procedures. This represents more than one order of magnitude improvement over predecessors and surpasses by far the EPRI ALWR URD goal of 1 x 10^{-5}/year.

2. DESCRIPTION OF 15 SPECIFIC DESIGN AREAS AS SELECTED FROM INSAG-3

In the following sections the reference to INSAG-3 is put in parentheses after each heading.

2.1. Plant process control systems (4.2.2.1)

The task of the open and closed-loop controls is to control power generation during normal operation and anticipated operational occurrences (start-up, shutdown, and power operation) such that predetermined setpoints for relevant process variables are reached and maintained.

In line with the fluid system structure the open and closed-loop control equipment for major process variables can be subdivided on the basis of their tasks:

- reactor coolant system controls,
- turbine controls,
- and other secondary side system controls.

Besides the above, there is a range of further I&C equipment which serves for open and closed-loop control of miscellaneous components in the water/steam cycle and in auxiliary and ancillary systems (general operations controls).

Reactor coolant system controls serve to regulate main process variables for the primary system. These variables are:

- average coolant temperature,
- neutron flux,
- control assembly position,
- coolant pressure, and
- pressurizer level.

The operational controls for the turbine generator and the overall feedwater/steam cycle are the following:

- turbine control system (with speed, load and main steam minimum pressure control loops),
- main steam bypass control,
- steam generator level control,
- condensate run-off control.

2.2. Automatic safety systems (4.2.2.2)

To mitigate the consequences of design basis accidents, Konvoi is equipped with a special safety system, consisting of the reactor protection system (RPS) and the engineered safety features controlled by it. The RPS is a safety grade instrumentation and control system which in case of violation of preset parameter limits initiates a reactor trip and actuates the engineered safety features.

In order to minimize the demand frequency of safety systems and to enable a smooth transient course in addition to safety systems operational systems are designed to fulfill safety tasks (e.g. start-up and shutdown system, in front of EFWS, boration by CVCS in front of extra borating system). These systems are of higher quality than pure operational systems including redundancy requirements and are foreseen for periodic testing.

This staggered concept is reflected too in the I&C structure by operational I&C, limitation functions and reactor protection system (see figures 4 and 5).

The following automatic safety systems are provided in the design

- reactor protection system,
- reactor trip system (control assemblies),
- extra borating system,
- emergency core cooling and residual heat removal system,
- emergency feed system and emergency generators (emergency power system no. 2),
- emergency diesel generators (emergency power system no. 1),

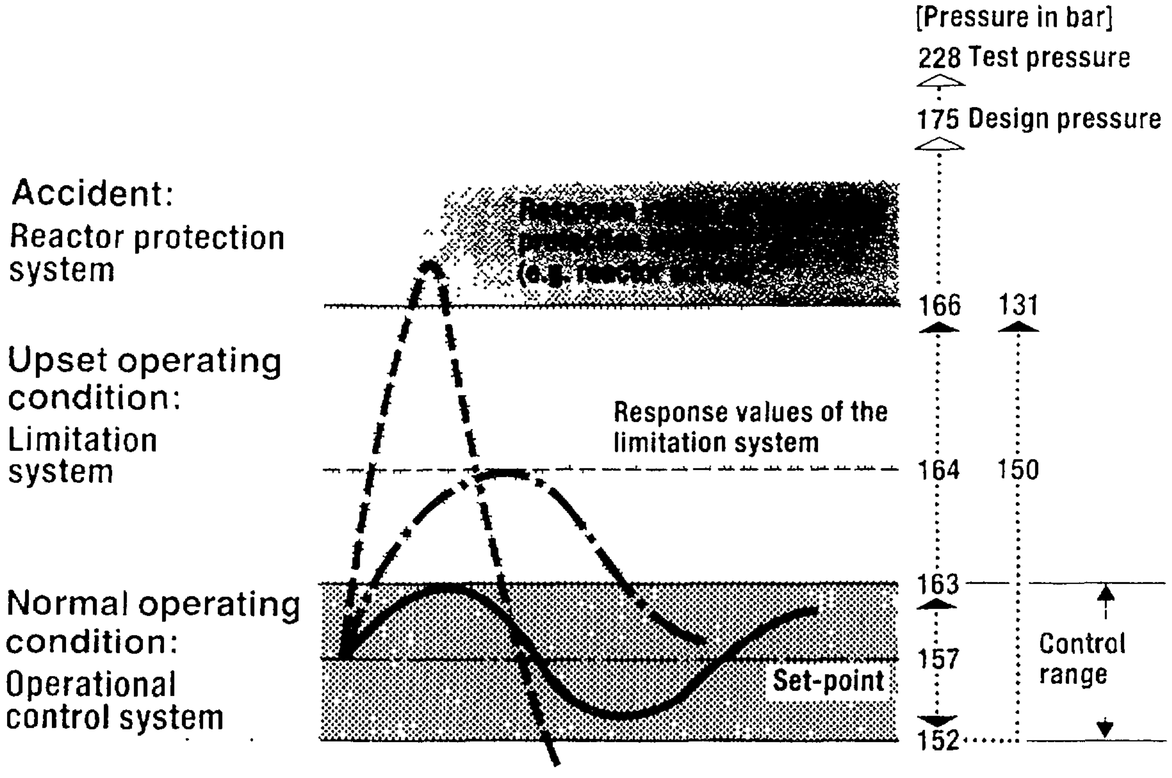

[Pressure in bar]
228 Test pressure
175 Design pressure
Accident:
Reactor protection system
(e.g. reactor
166
131
Upset operating condition:
Limitation system
Response values of the limitation system
164
150
Normal operating condition:
Operational control system
163
157
Set-point
152
Control range

Fig. 4: Control and Protection Levels (Reactor Coolant Pressure)

- component cooling system,
- secured closed cooling water system,
- service water system for secured plant,
- annulus air extraction system,
- containment isolation system,
- isolation of reactor cooling system,
- isolation of main steam and feedwater lines,
- main steam relief valve station.

2.3. Protection against power transient accidents (4.2.3.1)

Three independent reactivity control systems are provided. The first system consists of the control assemblies which serve to control and shutdown the reactor. On reactor trip, the control assemblies drop into the reactor core under the force of gravity. The control assemblies are operated in groups of four quadruplets which are actuated together but can also be operated individually. The quadruplets are assigned to the L or D-bank. The two banks effect the required load changes by changing the overall reactivity of the reactor. Reactivity feedback effects of fuel temperature and coolant temperature can be compensated for by changing the D-bank position. In the event of rapid and large load changes the position of the L-bank is adjusted. The system is capable of holding the reactor subcritical with sufficient margin in hot-standby conditions (296°C) and down to about 250°C reactor coolant temperature (200°C without stuck rod).

The second system, the chemical volume and control system (CVCS) is an operational system which has the task - among others - to inject boric acid and demineralized water into

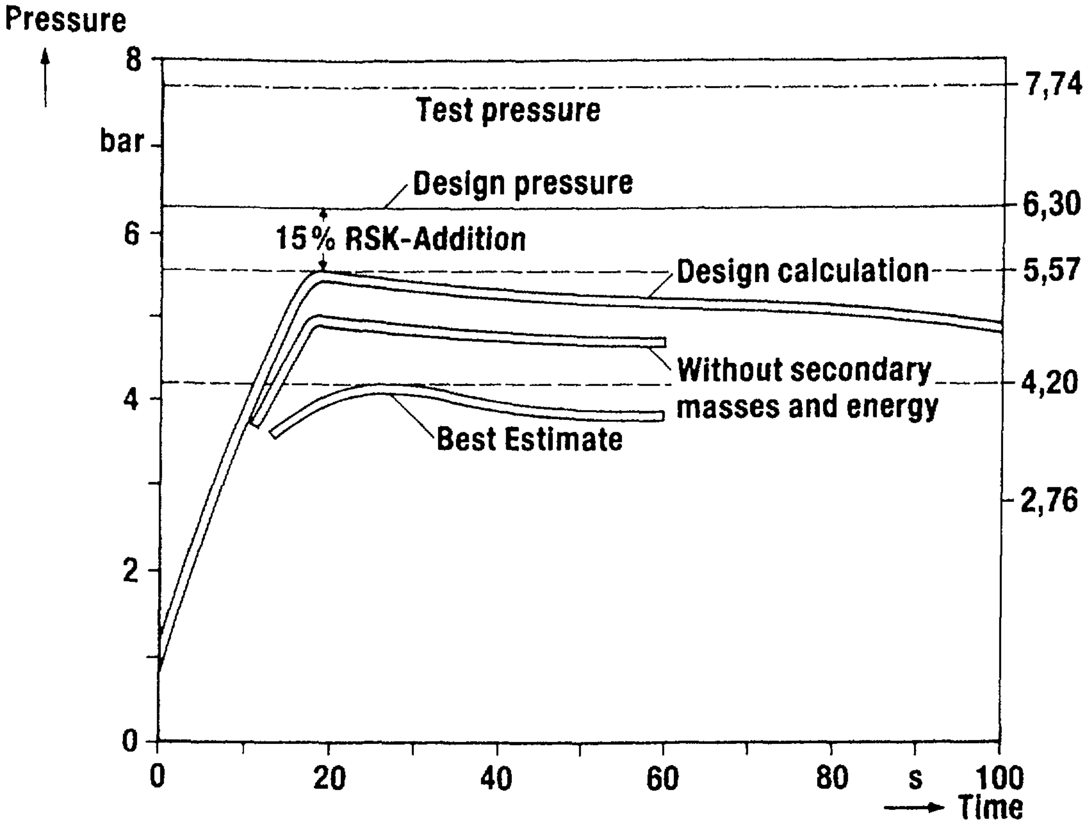


Fig. 5: Cumulative Safety of Pressure Related Design

the reactor coolant system as necessary for chemical reactivity control and discharge letdown coolant into the coolant storage tanks. This system is not required for design basis accident control, but when available it is used so as not to call upon the safety systems (see 2.2). Therefore, to ensure continued operation of the CVCS in emergency power operation, all three pumps and motor-operated valves are connected to emergency supply system no. 1 (isolation valves between reactor coolant and volume control system are connected to emergency power supply system no. 2 and thus supplied by both emergency power supply systems).

In addition, a third system, the extra borating system (see 2.2) as safety system is provided. This system shuts down the reactor and keeps it in a long-term cold subcritical and xenon-free condition together with the control rods if the CVCS is not available.

2.4. Reactor core integrity (4.2.3.2)

The reactor core is designed to comply with appropriate margin with the German codes and standards to ensure that design criteria during any condition of normal operation, including the effects of anticipated operational occurrences are fulfilled. The design criteria include:

- The minimum departure from nucleate boiling ratio during normal operation and anticipated operational occurrences will provide at least a 95% probability with 95% confidence that departure from nucleate boiling does not occur.
- The maximum fuel centerline temperature must be lower than the meltdown temperature of the fuel.
- Fuel rod cladding is designed to maintain cladding integrity throughout fuel life.
- The reactor system is designed so that any xenon transients will be adequately damped.
- The reactor is designed such that the combined response of the fuel temperature coefficient, the moderator temperature coefficient, the moderator void coefficient, and the moderator pressure coefficient to an increase in reactor thermal power is a decrease in reactivity. The reactor is designed such that the moderator temperature coefficient is negative at all power levels throughout the entire operating cycle. In addition, reactor power transients remain bounded and damped in response to any expected changes in any operation variable.
- The RCS is designed and constructed to maintain its integrity throughout the expected plant life. The reactor and the I&C, staggered into control, limitation, and reactor protection system are designed such that power excursions that could result from any credible reactivity addition incident do not cause damage, either by deformation or rupture of the pressure vessel, or impair operation of the engineered safety features.

2.5. Automatic shutdown system (4.2.3.3)

The reactor protection system (see 2.2) is designed to rapidly shut down the reactor when certain plant conditions approach safety system setpoints. The system monitors plant condition to actuate a reactor trip in response of the following safety parameters or a combination thereof:

- neutron flux density
- relative rate of change in neutron flux density > max.
- reactor thermal power
- corrected reactor thermal power
- sliding power limit
- DNB ratio
- reactor coolant pump speed
- average coolant temperature
- reactor coolant system pressure
- pressurizer level
- containment pressure
- steam generator level too low
- main steam pressure too high
- main steam pressure gradient
- radioactivity in main steam line
- control assembly busbar voltage level too low
- (manual trip)

2.6. Normal heat removal (4.2.3.4)

The residual heat removal systems used for shutdown of the plant comprises on the primary side the emergency core cooling and residual heat removal systems including residual heat removal chain, and on the secondary side the following systems:

- start-up and shutdown piping system
- emergency feedwater system
- main steam valve station consisting of main steam safety and relief control valves for steam release to the atmosphere
- turbine bypass station inclusive of the associated auxiliary systems.

During normal operation and anticipated operational occurrences the secondary side is used to cool the reactor coolant system down to RCS conditions below 180°C using the steam generators. The primary side is subsequently used to provide cooling by the ECC and RHR system and transfer the reactor system to the cold depressurized condition and maintain this condition in the long-term (in addition, fuel pool cooling is performed).

Starting from the zero load condition, decay heat and stored heat are transferred via the steam generators to the steam/power conversion system. Turbine control valves are closed, and the generated steam is directed to the turbine condenser via the turbine bypass station. Subsequent shutdown to cold subcritical condition is performed via steam generators and condenser until coolant temperature has fallen to about 120°C. Then heat removal via steam generators is stopped and further cooldown is performed by ECC and RHR system. The procedure to reach the cold subcritical state starting from zero load condition is specified to be performed within less than 12 hours.

2.7. Emergency heat removal (4.2.3.5)

The residual heat removal systems outlined in 2.6 are also used for heat removal in case of transients and LOCAs, and fulfill the following tasks:

Transients

Secondary side:

- to feed the generators on loss of normal feedwater supply;
- to dump the resulting steam on loss of main heat sink;
- to cool the reactor coolant system as necessary down to RCS conditions below 180°C using the steam generators

Primary side:

- to provide cooling by the ECC and RHR systems after cooldown by the steam generators, to transfer the reactor system to the cold depressurized condition and maintain it in this condition in the long-term;
- to cool the fuel pool.

Small-break LOCAs

Secondary side:

- to feed the steam generators and dump steam on loss of main heat sink;
- to cool the reactor coolant system automatically at approximately 100 K/h down to below 180°C using the steam generators;

Primary side:

- to maintain the reactor coolant system water level by injecting borated water;
- to provide cooling by the ECC and RHR system after cooling by the steam generators, to transfer the reactor system to the cold depressurized condition and maintain it in this condition in the long-term;
- to recirculate the coolant from the containment sump into the reactor coolant system.

Medium-Break and Large-Break LOCAs

Primary side:

- to reflood the reactor core and maintain the reactor coolant system level;
- to cool the coolant in the residual heat exchangers and return it to the reactor coolant system;
- to keep the reactor system in the cold depressurized condition on a long-term basis.

Accidents due to External Events, Concurrent with Loss of Auxiliary Power Supply and Emergency Power Supply System No. 1

Secondary side:

- to feed the steam generators and dump the steam to maintain the shutdown reactor system in the hot subcritical condition for 10 hours;
- to cool down the reactor system to RCS conditions below 180°C within max. 10 hours, using the steam generators;

Primary side:
- to provide cooling by the ECC and RHR system after cooldown by the steam generators, to transfer the reactor system to the cold depressurized condition and maintain it in this condition in the long-term;
- to cool the fuel pool.

For description of the engineered safety features of heat removal system, see section 2.2.

2.8. Reactor coolant system integrity (4.2.3.6)

The reactor coolant system consists in essence of:

- the reactor pressure vessel;
- four steam generators;
- four reactor coolant pumps;
- the connecting reactor coolant piping;
- the pressurizer;
- the pressurizer relief tank complete with cooling system; and
- pressurizer spray valves, relief valves and safety valves.

The reactor coolant pressure boundary is designed to accommodate the system pressures and temperatures attained under all expected modes of operation, including all anticipated transients and maintain the stresses within acceptable limits.

The base metal used for the reactor coolant pressure boundary is the low-alloy, heat-resistant, fine-grained structural steel 20MnMoNi55. All coolant-wetted surfaces are protected against corrosion by means of an austenitic weld overlay cladding. Exceptions to this are the piping connected to the RCL and the pressurizer relief tank which are made entirely of austenitic steel.

In accordance with German regulations requirements are fulfilled which justify the "break preclusion" concept.

By use of high quality fabrication methods and avoidance of longitudinal welds, the total number of welds is reduced drastically from about 240 in previous designs to 60.

The required pre-service inspections (material testing, final inspection and pressure testing) as well as in-service inspections (ultrasonic, eddy current examination, surface crack examination integral testing) and integrity monitoring by leakage monitoring system, loose part monitoring system, vibration monitoring system and fatigue monitoring system is performed.

Overpressure Protection

Pressurizer heating and spraying, and response of the relief valve are triggered at step-raised setpoints on either side of the steady-state operating pressure. Above this range the safety valves respond to protect the reactor coolant system against unacceptable overpressures.

The relief valve and the safety valves are opened by means of pilot valves at fixed pressures. Additional bleed valves in the pilot system permit the relief valve and the safety valves to be opened at a lower pressure in the course of emergency procedures.

The steam generators are vertical U-tube natural circulation heat exchangers. The hemispherical channel head at the bottom is divided into an inlet and an outlet channel and welded to the tube sheets above. To reduce the number of welds, the parts of the pressure retaining boundary are fabricated from seamless cylindrical forgings made of 20 MnMoNi55. For the steam generator tubes Incoloy 800 modified is used. Many years of positive operating experience have proven that Incoloy 800 in this modified composition fulfills the requirements for high corrosion resistance.

An increase in radioactivity indicated by main condenser evacuation system monitor, and blowdown system monitors will reveal reactor coolant leakage through steam generators tubes to the secondary side. Routine analysis of steam generator secondary water samples will also indicate increasing leakage of reactor coolant into the secondary system. Additionally, the Konvoi design incorporates four N-16 monitors, one per steam generator, to provide a sensitive and specific indication for primary coolant leakage through steam generator tubes.

2.9. Confinement of radioactive material (4.2.3.7)

The confinement envelope (see fig. 1) consists of:

- the spherical steel containment, including air locks and penetrations for pipes, cables and air ducts;
- the isolating valves in the piping and air ducts that penetrate the containment wall;
- the surrounding reinforced concrete outer shell and basement;
- the leak-off system and annulus air extraction system for retaining and filtering any leakages from the containment; and
- the venting device in order to preclude containment overpressure failure in case of core melt situations.

The function of the confinement envelope is essentially to protect the environment against the unacceptable release of radioactive materials under all postulated accident conditions. A design leak rate of 0.25 Vol%/day is specified for the steel containment. Tests reveal that the real leak rate is much lower.

The break cross section of up to 2A in the reactor coolant lines must be assumed as the basic for determining the design pressure of the containment. This maximum accident pressure is also based on the assumption that, during reactor coolant blowdown the entire energy and mass contents of the secondary side of one steam generator are released into the containment including the main steam line up to the first isolation valve (see figure 5).

Piping penetrations that are not associated with the safety systems are double isolated (one isolation valve located inside and outside the containment).

The outer concrete shell is designed to protect the containment against external events (safe shutdown earthquake, fast military airplane crash, explosion pressure wave). In addition, it protects the environment against line-of-sight radiation from radioactive reactor coolant in the event of a loss-of-coolant accident.

Each door of all the personnel and equipment air lock is designed to withstand the same pressures and temperatures as the containment itself.

In normal operation the division of the reactor building into compartments and the associated HVAC systems ensure that prescribed air conditions are maintained and that air flows from less radioactive to more radioactive compartments in order to prevent the spread of radioactive materials.

This ensures that the small equipment compartments are accessible under certain conditions and service compartments are generally accessible during normal operation. In the event of accidents involving positive pressure in the containment, air is removed from the annulus by the annulus air extraction system, creating a negative pressure in the annulus which prevents the escape of radioactive materials to the environment through the outer concrete shell which is not gas-tight. The radioactive materials are removed from the extracted air by filters and the air is expelled through the vent stack.

Certain enclosed piping penetrations are nitrogen-filled which permits them to be checked for leak-tightness. In the event of an accident, the leakage can be extracted from the space between the double seals of air locks and air duct dampers by the leak-off system and transferred back into the containment.

Some of the concrete and steel interior structure of the containment serve to protect the containment against missiles and the loads arising from differential pressures in the event of an accident. On loss of coolant accident initiation, all penetrations that are not associated with the safety system are isolated by the safety I&C system. Parts of the safety system are isolated separately, where this is necessary or practical for specific accident sequences. The filtered containment venting device is foreseen to avoid overpressure failure of containment in case of severe accidents.

2.10. Protection of confinement structures against internal and external events (4.2.3.8)

The topic has been treated in the previous section.

2.11. Monitoring of plant safety status (4.2.3.9)

The control room serves as the central control station for the power plant. It accommodates the operator control and information display equipment for control and monitoring of the unit; manual control, parameter setting and monitoring of the nuclear steam supply system, reactor auxiliary systems, water/steam cycle, turbine, generator and auxiliary power systems are performed as necessary in the control room.

Apart from this, instrumentation and recording equipment used during and after accidents and in unforeseeable event sequences is also installed in the control room complex to:

- supply sufficient information on the condition of the plant to enable the necessary measures for the protection of staff and the plant to be taken;

- indicate and record the course of events; and
- allow estimation of any effects on the environment.

The equipment of the central control room conforms to the requirement that the I&C systems of a nuclear power plant have to be highly automated.

The protection systems, i.e. systems which take priority over manual actions and over the operational controls, are provided for the safety of staff, environment and of the entire plant; they comprise the reactor protection system, the limitation system and the equipment unit protection systems.

The reactor protection system signals and thus the automatically initiated actions override manual actions taken in the control room and the remote shutdown station.

The indicators for measured data from the power plant process are accommodated in the area of the associated operator control equipment for those systems of the plant which are represented on the master or systems control console. They provide information on the overall plant condition.

2.12. Preservation of control capability (4.2.3.10)

The remote shutdown station housed in the emergency feed building serves the purposes of cooldown of and residual heat removal from the reactor coolant system after loss of control room function (e.g. after an external event) unless this is automatically activated by the reactor protection system.

The remote shutdown station is completely independent of the control room. The remote shutdown station and the four redundancy sections of the emergency feed building accommodate the following systems:

- control and indication equipment of the emergency feed system;
- associated I&C systems;
- that part of the reactor protection system which initiates the required measures under emergency feed conditions;
- the control systems of components which have to operate under emergency feed conditions or on external events during refuelling; and
- I&C systems necessary for operability and monitoring of relevant components.

All power supplies in the emergency feed building are of four-train configuration.

2.13. Station Blackout (4.2.3.11)

The power supply from either the main grid of the generator itself (easy load rejection to house load) or via the standby grid leads to high reliability for the normal power supply system. This is reflected in the German experience which shows that duration of emergency power modes (EPM) is well below 2 hours.

To cope with the EPM requirements, Konvoi is equipped with 2 independent emergency power supply systems to cover among others the common mode failure or simultaneous destruction of the emergency diesels. This is fulfilled by provision of redundant and diverse emergency power supply systems consisting of four emergency diesel generators designed for the emergency power mode and serving the emergency power supply grid D1 **and** four additional, diverse diesel engines driving directly the emergency feedwater pumps. These smaller diesel engines drive additionally four generators serving the emergency power supply grid D2.

Emergency power supply system 1 is connected in particular to those loads which are required to control design basis accidents, transients and loss of coolant accidents and to subsequently inject water into the reactor coolant system.

Furtheron, a third grid connection (subterranean) is provided which is capable of taking over the loads from the emergency power supply system no. 1, thus relieving the diesel generator set from lengthy operation.

Emergency power supply system no. 2 is connected to those loads which are required for control of accidents caused by external events such as aircraft crash or explosion blast waves. Consequently all electrical components of emergency power supply system no. 2 are designed to withstand the postulated external events and are installed in the emergency feed building which also withstands these loadings.

The power required for the loads of emergency power supply systems no. 1 and no. 2 is mainly provided by the plant auxiliary power supply system. The auxiliary power supply system to which no loads important to safety are directly connected is supplied from the national high voltage power system or the plant generator via the main or alternative offsite grid connection. On loss of power from all of these sources for the auxiliary power supply system the four-train emergency diesel generator sets take over power supply to emergency power supply systems no. 1 and no. 2. If emergency power supply system no. 1 fails, the four emergency feedwater diesels drive directly the associated generators supplying the D2 net.

In addition, the uninterruptable battery supply is provided to supply the safety-related instrumentation for at least 2 hours without the need of refeeding the batteries.

2.14. Control of accidents within the design basis (4.2.3.12)

The NPP is built in such a way that the three basic safety goals:

- safe shutdown and maintained shutdown condition;
- residual heat removal; and
- radiation exposure of the personnel and the environment below prescribed limits,

are fulfilled in case of transients and accidents.

For practical reasons these basic safety goals are split into seven safety goals to which safety functions fulfilling these specific goals are assigned to. To specific safety functions the systems foreseen are assigned:

2.15. Mitigation and control of severe accidents (4.2.3.12)

A severe accident is one that involves appreciable core damage. The Konvoi design represents a resilient plant design not only to prevent core damage but also to moderate the severity of such an accident should one occur. This is the function of the containment and the systems that support it. A 56 m diameter and about 71000 m^3 of free volume allow cost effective innovation to directly address severe accident concerns.

Prerequisite to carry out mitigating procedures (maintain the integrity of the previously isolated containment and to permit only controlled and filtered radioactivity release) is to transfer the plant from a possible high pressure RPV melt-through to a low pressure core melt sequence to avoid early containment failures. This is performed by prior RCS bleed via highly reliable pressurizer valves.

Then adequate time is available for further procedures to avoid containment failure due to:

- formation and explosion of hydrogen in the containment, or
- long-term pressure build-up.

To cope with the hydrogen problem, a dual concept consisting of hydrogen igniters and recombiners is foreseen.

To avoid containment failure by long-term pressure build-up due to mass and energy input at reaching the test pressure of the containment after several days a system for filtered venting of the containment atmosphere to the vent stack is provided. The venting system is designed to restrict the containment to test pressure without water needing to be injected into the sump and combined with water injection into the sump, to reduce the containment to half the test pressure within two days provided that venting is initiated every time test pressure is approached.

If further Konvoi plants were to be built in future, in addition the design is changed to provide a spreading area of about 100 m^2 for core melt. This was conceptually developed for the bid for the fifth NPP unit in Finland.

3. EXTENDED DATA LIST

Station output

Rated thermal power of reactor	3,782 MW
Net electrical output	1,287 MW

Fuel assembly

Array	square (18 x 18-24)
Number of rod fuels	300
Number of guide tubes for absorber/ in core instrumentation	24
Full length (without control spider)	4,827 mm
Fuel rod:	
- length	4,402 mm
- outside diameter	9.5 mm
- cladding material	zircaloy 4
- cladding thickness	0.64 mm
- initial internal pressure (He)	22 bar (2.2 MPa)
Fuel pellet:	
- material	UO_2
- density (percentage of theoretical density)	10.4 g/cm^3
- length	

Reactor core

Number of fuel assemblies	193
Active height	3,900 mm
Equivalent diameter	3,605 mm
Rod cluster control assemblies absorber:	
- number of assemblies	61
- absorber rods per assembly	24
Enrichments:	
- first core	1.9; 2.5; 3.2%
- reload	3.2; 3.4%
(H_2O/UO_2) volume ratio (cold)	2.09
Average fuel burn-up	31,800 MWd/t
Total weight of U	103 t

Reactor coolant system

Design conditions:	
- pressure	175 bar (17.5 MPa)
- temperature	350°C

Operating pressure	157 bar (15.7 MPa)
Temperature difference vessel inlet/outlet	34.8°C
Flow rate	18,800 kg/s
Heat transfer surface in core	6,036 m^2
Mean spec. rod power	163 W/cm
Mean spec. power output of fuel	93 kW/kg

Reactor vessel

Overall height	11,775 mm
Inside diameter	5,000 mm
Wall thickness (opposite the core)	250+6 mm
Minimum stainless steel cladding thickness	6 mm
Inlet/outlet nozzle inside diameter	750/755 mm
Mass (excluded head)	370 t
Material (forged rings)	20MnMoNi55
Design pressure/temperature	175/350 bar/°C
Neutron fluence for service life (E - 1 MeV)	5 x 10^{18} n/cm^2

Reactor coolant pump

Type	single-stage centrifugal pump
Number	4
Design pressure/temperature	175/350 bar/°C
Design flow rate	4,700 kg/s
Pump casing material	20MnMoNi55 (forged)
Speed	1,480 rpm
Power at coupling, cold/hot	7,350/5,430 kW
Weight	110 t
Cost down time	330 s

Steam generator

Type	U-tube heat exchanger
Number	4
Heat transfer surface	5,400 m^2
Number of heat exchanger tubes	4,100
Tube dimensions	22 x 1,2
Outside/inside diameter of shell	4,812/ mm
Total height	21,320 mm
Transport weight	420 t
Shell and tube sheet material	20 MnMoNi55
Tube material	Incoloy 800
Steam pressure at SG outlet	63.5 bar (6.35 MPa)
Steam output	513 kg/s
Feedwater temperature	218°C
Water volume of secondary side	63/116 m^3

Steam moisture at outlet from SG	0.25%

Pressurizer

Total volume	65 m^3
Steam volume; full power/zero power	26.6/41.8 m^3
Design pressure/temperature	175/350 bar/°C
Heating power of the heaters	2,000 kW
Number of heaters	102
Outside/inside diameter	2,882/2,600 mm
Total height	13,200 mm
Material	20MnMoNi55
Transport weight	140 t

Containment

Configuration (single or double)	double
Material	15MnNi63
Gross volume	ca. 71,000 m^3
Design pressure/temperature	5.3/145 bar/°C
Height/diameter	56 m
Design leak rate	< 0.25 Vol %/day

BASIC INFORMATION ON DESIGN FEATURES OF THE N4 NUCLEAR POWER PLANT

J. P. BERGER, B. PERRIN
Electricité de France (EdF),
Villeurbanne

D. LANGE
FRAMATOME,
Paris

France

Abstract

The paper describes the N4 nuclear power plant design of Framatome, France. The paper consists of three parts: - a general description; - a description of how the plant compares with the safety principles of INSAG-3 for 15 selected design areas; and - an extended data list. The general description outlines the French general safety philosophy, and describes the N4 design, the main features of the reactor plant and its safety systems. The second part discusses plant performance in the areas of: - plant process control systems; - automatic safety systems; - protection against power transient accidents; - reactor core integrity; - automatic shutdown systems; - normal heat removal; - emergency heat removal; - reactor coolant system integrity; - confinement of radioactive material; - protection of confinement structure; - monitoring of plant safety status; - preservation of control capability; - station blackout; - control of accidents within the design basis; and - mitigation and control of severe accidents. The third part, finally, presents data related to the power plant as a whole, data on the containment, on the reactor coolant system, the reactor pressure vessel, steam generators and pressurizer, and on reactor core and reactivity control.

1. GENERAL DESCRIPTION

1.1. Introduction

The French N4 plant is a 1400 MWe PWR standard series, whose first unit Chooz B-1 is to be commissioned in early 1995. As regards safety, it has been designed in an evolutionary perspective, taking benefit of the experience gained on the previous standardized series of 900 MWe and 1300 MWe plants, and keeping open to technological progress and new developments after careful validation.

Of course, the N4 plant has inherited the sound safety bases common to all Western PWRs; the implementation of the defense-in-depth and multiple barrier concepts, the design of the plant for a specified list of design basis conditions, the protection against internal and external hazards, and the use of conservative deterministic rules for design, construction and safety evaluation. However, a number of technological improvements and innovative features have been implemented in the N4 plant design.

The aim of this paper is to remind briefly the French safety general philosophy, to illustrate through a general description of the plant (see also attached Figures) the way that philosophy has been implemented, and to describe the selected 15 key design areas from INSAG-3.

1.2. French safety general philosophy

The implementation of France's major nuclear programme - 54 PWR units in service - has gone hand in hand with the development of an original philosophy in the field of nuclear safety. This philosophy combines two essential elements which have shaped this nuclear programme:

1) Whilst the French units were originally built under license from an American manufacturer (Westinghouse for the nuclear steam supply system), the design of these plants has been progressively made French. In terms of nuclear safety, this French influence has led to further development of the deterministic design approach current in the United States to include consideration of a number of additional situations based on a probabilistic approach. This has resulted in a better coherence for safety.

2) Electricité de France performs the dual role of both operator and industrial architect of its power stations. This has resulted in an active commitment to safety in service, utilizing the feedback of operating experience at a very early stage in the design, and also by improving the design with a view to enhancing operational safety (man-machine interface, operating procedures).

Furthermore, the establishment of emergency plans has enabled the Safety Authority and the operator to adopt a coherent and logical approach to the severe accidents which may call for the implementation of these plans. With the aim of achieving greater defence in depth, this has resulted in the provision of certain additional measures designed to further reduce the probability and consequences of severe accidents.

Thus, from an initial core of deterministic safety philosophy developed across the Atlantic, and which has been wholly retained and in some instances refined, a range of additions have been made which enhance the overall level of safety of the installations without undue complication.

1.2.1. A deterministic design philosophy

EDF's design philosophy hinges on the two basic principles of prevention and control of accidents. To this end, the philosophy is based on the concept of defence in depth, at three levels:

Level 1:

Every precaution is taken to ensure that the unit is fundamentally safe: quality of design studies (incorporating adequate safety margins), quality of construction and associated testing inspection.

Level 2:

Safety systems and protection systems detect and arrest the development of incidents which can lead the unit out of its normal operating range.

Level 3:

It is further assumed that hypothetical accidents liable to compromise the containment of radioactive substances may occur.

In order to guard against these accidents, safeguard systems are designed together with that of the protection system enabling their use which operate to limit the consequences of such accidents to an acceptable level.

In practical terms, this deterministic approach to safety operates on the following principal lines:

a) Establishment of a list of events of internal origin liable to occur during the life of the installation, which may be of a hypothetical nature, classified into categories according to their estimated probability of occurrence where this can be assessed: the design operating conditions.

b) Selection within each category of so called "envelope"-events, having regard to their consequences which should predominate over those of the other events in the same category, also referred to as design operating conditions.

c) Design and rating of the various buildings, structures, systems and equipment so as to afford protection against the effects of the various events selected, followed by a study of their consequences using a number of deterministic conventions:

   - single failure criterion,
   - adoption of the principle of geographical or physical separation of redundant equipment,
   - independence of power sources, and of their distribution,
   - accident studies conducted using pessimistic assumptions and conservative calculation rules.

d) Allowance in the design for the existence of hazards of internal origin:

   - internal projectiles,
   - high energy pipe breach,
   - internal flooding,
   - fire.

e) Allowance in the design for the existence of hazards of external origin:

   - hazards of natural origin: earthquakes (the standard design spectrum in the horizontal spectrum of the R.G. 1.60 issued by NRC calibrated to 0.15 g), continental and marine flooding, extreme meteorological conditions,
   - hazards related to human activity: aircraft crashes, industrial environment and lines of communication (explosions, fires, toxic gases).

For this last type of hazards, Basic Safety Rules define a probabilistic objective of safety, which specify the upper limit of probability of an unacceptable release of radioactive substances at the site boundary at some 10^{-7} per year, per unit, per safety function and per category of hazards. A risk of probability below this limit will be referred to as "residual risk". The basic principle for protection of power stations against this type of hazard involves the use of constructional arrangements designed to reduce the risk to this residual level.

1.2.2. Contribution of the probabilistic tool

However, although providing appreciable margins for the envelope cases treated, it is clear that the deterministic method, whilst highly effective for design purposes, has the basic flaw of being restrictive, which poses a number of questions relating to safety analysis:

- is the list of operating conditions defined at any given moment sufficient and truly all embracing?
- is it acceptable to lose safety systems designed according to this methodology (and so to go beyond the single failure-criteria)?
- does this philosophy actually result in a coherent design of the unit in terms of safety?

The answer to these questions may be found first and foremost in the different utilizations of probabilistic studies:

- design aid: through an extensive programme for methods development, data acquisition and detailed reliability analysis of safety systems,
- study of external events due to human activity,
- verification of design coherence through probabilistic safety assessments (PSAs).

The French safety authority has set the following objective: a new PWR unit should be dimensioned so that the overall probability of unacceptable consequences does not exceed 10^{-6} per year.

To respect this overall risk objective, the probability that a family of events will lead to unacceptable consequences must not exceed 10^{-7} per reactor per year.

Furthermore, the probabilistic safety assessment (PSA) permitted to identify conditions at the boundary of the design basis which deserved the greatest attention.

It was therefore decided to add to the list of design conditions, a number of complementary design conditions, corresponding mainly to the total failure of redundant systems.

The main analyzed complementary design condition are the following ones:

- total loss of ultimate heat sink,
- total loss of feedwater in steam generators,
- total loss of electrical power supplies,
- reactor trip system failure (ATWS),
- total loss of low head safety injection or containment spray during the long term after LOCA,
- concurrent rupture of main steam line and one or more SG tubes.

For each of these conditions, the objective is to demonstrate that the main safety functions (subcriticality, core cooling, containment) are maintained, using either available systems or specific complementary mitigating means.

In case such complementary means are introduced, they must be designed for simplicity, and, as far as possible, diversity with regard to the system backed up.

1.3. Design of the N4 plant

Since the Three Mile Island accident, significant improvements have permanently been made to reduce the probability of core melting; they have led to the design of the N4 plants; we will only present the most significant features of that series.

1.3.1. Safety: Imagine the worst to better prevent it from happening

a) Designing the systems important for safety to be simple, redundant, and diversified.

1) One function per system

Multifunction systems are avoided and each safety function is ensured by a single system. This design presents three advantages:

- it is unnecessary to modify the configuration of the systems in case of an accident,
- system operation is simpler, therefore easier to understand for the reactor operators,
- the reactor operators can more easily predict system behavior.

2) "Two-train" systems

All fluid systems important for safety have two redundant subsystems, called "trains". This concept presents the following advantages:

- the ratio of the safety level to the corresponding investment is excellent,
- it is easier to install the piping and equipment,
- the interfaces between the reactor building, the safeguard and the auxiliaries building can be created with great flexibility,
- maintenance is greatly facilitated.

3) Diversification of backup means

Accident sequences that include multiple failures go beyond the single failure criterion. To account for this, diversified backup systems have been installed, in the short term for frequently used systems and the long term for systems used infrequently.

b) Defense in depth to limit the risks and consequences of severe accidents.

Severe accidents include situations that lead to draining of the reactor coolant system, followed by core melt. The melted core, called the corium, may burn through the reactor vessel and flow into the bottom of the reactor containment.

The result is a large release of radioactive fission products inside the containment and possibly into the environment, if confinement inside the containment is not ensured.

For the N4 units, application of the defense-in-depth principle (previously described) has enabled to meet the objectives set by the French Safety Authority. To limit the severe accident risks and consequences:

- prevention is ensured by keeping the essential safety functions operational,
- accidents are managed to alter their sequences and stop them from becoming worse, and
- the consequences of core melt are limited by applying an off-site emergency environmental protection plan.

1) Preventing core melt

To deal with complementary design situations, some procedures have been implemented:

H1: Total loss of heat sink,
H2: Total loss of steam generator feedwater,
H3: Total loss of electrical power supplies (off site and on site), and
H4: Mutual backup between the containment spray system and the low pressure safety injection system, complemented by procedure U3 for setting up mobile equipment to make this possible, including pumps, heat exchangers, and interconnecting piping.

2) Improving the management of severe accidents by means of a physical condition approach.

The post-accident operation of PWR units has been subjected to a general review. During this reexamination, the following actions were taken:

- the incidents and accidents that have occurred on French and foreign nuclear power units were analyzed,
- account was taken of the experience acquired during training on site and on plant unit simulators.

Event oriented operating procedures - based on identification of the initiating event - cannot take into account all possible combinations of events. Therefore, a new operating method has been implemented that is based on the physical status of the NSSS and of the main systems. This type operation depends on the parameters that characterize the instantaneous condition of the NSSS. It enables bringing the unit to a safe shutdown condition without having to make any hypotheses on the initiating event, while continually updating the diagnosis and the necessary actions.

All post-accident procedures are written in accordance with this "**physical state approach**".

3) Limiting the radiological consequences

Under the hypothesis that a core-melt accident cannot be avoided, it is the ultimate performance of the confinement barrier, in this case the reactor building, that is crucial. Measures have been taken to safeguard the integrity of the reactor containment and to limit the release of radioactivity into the environment.

The operating guide for severe accident situations defines, for the operating utility, the actions to be taken in post-accident operation following a core melt accident.

In view of the instrumentation dispositions taken and the present state of knowledge about the physics of severe accidents, complemented by the results of analyses and R&D, the objectives are as follows:

- to prevent or minimize radiological releases into the atmosphere or ground water,

- to gain time for implementing an emergency response plan, and
- to return the unit to a more easily controlled status.

Special so-called ultimate procedures ("U"-procedures) are implemented, complementing the accident mitigation means, to:

- limit the pressure buildup inside the containment and the releases to the environment (procedure U5), by means of a venting system fitted with a sand filter;
- limit the radioactive releases by precipitating the fission products out of the containment atmosphere, while preventing bypass, and by applying procedure U2, which aims to locate and stanch the radioactive leaks;
- cool the corium and slow down the erosion of the reactor building basemat; and
- put a stop to the aggravation of the accident by means of special measures: dropping the reactor coolant system pressure and using borated water.

1.3.2. Feedback from operating experience

A considerable experience was gained in the past fifteen years in France with the operation of the 900 MWe and 1300 MWe standardized series.

As an example, the ΔT measurement bypass which permitted to measure temperatures of the reactor coolant system, and which revealed to highly contribute to the doses to the operating staff, were all removed and replaced, on the N4 plant, by temperature detectors directly mounted on the pipe.

The experience feedback was also directed to the analysis of current incidents which generally have no impact on safety but could be precursors of more safety-related incidents if concurrent failures occurred. In that matter, attention was given to the following two types of events:

Steam Generator Tube Rupture (SGTR) accident

Several actions were taken on the N4 steam generator materials, design, and equipment to reduce the likelihood of a SGTR incident. Also an improvement, permitting an early detection of the incident, was made through the installation of N-16 instrumentation on all steam lines.

In addition, progress in the mitigation of SGTR was introduced with the aim of maintaining the integrity of the secondary systems (avoiding contaminated release) as far as possible.

Moreover, to limit the risk of water discharge through the safety valves, a redundancy of the atmospheric dump system is implemented; each steam generator is equipped with two redundant safety-grade lines, each having a discharge valve and an isolation valve qualified for water discharge.

Incidents occurring at reactor shutdown

The PSA performed on the French 1300 MWe plants has highlighted the fact that risk at shutdown conditions, is for Western-type PWRs, not negligible, as generally believed.

Two kinds of sequences were shown to be potential contributors to core melt:

- loss of residual heat removal at "mid-loop operation" (frequent incident precursors have occurred world-wide)
- sudden dilution by water plug injection (here, no precursors ever occurred, since it is a rather unlikely condition).

Mid-loop operation consists in lowering the water level down to the RCS pipe level to facilitate certain maintenance operation. In this condition, the water level has to be monitored carefully: as loss in the RHR pump suction could lead to loss of heat removal and then to core uncovery in the most adverse conditions.

To lower these risks, the following improvements were provided:

- introduction of a permanent, integral level-measurement system covering the whole range of RCS water level, complemented by an accurate, ultrasonic RCS loop level measurement device for mid-loop operation,
- vortex detection,
- finally, a mitigation for the loss of heat removal is introduced: a make-up of borated water can be automatically actuated.

Sequences of reactor coolant dilution were also reviewed and an automatic action, cancelling any dilution in progress in case of loss of reactor coolant flow, has been introduced.

1.3.3. Increasing instrumentation and control safety, thanks to ergonomy and computerized information processing (see also paragraphs 2.11 and 2.14)

The fully computerized N4 control room allows the same functions as a conventional one. In addition, it considerably improves the man-machine dialogue in the operating and monitoring functions, in particular, when incident and accident phases are concerned.

a) Reducing the risks due to human factors

"Reducing the risks due to human factors by improving the quality of reactor operation, through actions affecting the design of the control room" was the objective set by EDF when the design of the N4 control room and the instrumentation and control system was initiated.

The following objectives were met:

1) reducing the quantity of information presented to the reactor operators and increasing its quality and pertinence;
2) improving the data processing and presentation, to facilitate its comprehension and use;

3) reinforcing communication between the operating and maintenance personnel, to better take into account during unit operation the actions of the maintenance departments; and
4) developing operating assistance information technology.

b) A control room that increases the reliability of the operating crew

Operation is normally accomplished under all situations using computerized control consoles. This choice makes available to the operators:

- the same means of unit operation in all situations, and
- means of information and control that offer flexible access to data and controls, without any rigid and hierarchical mechanism.

The computerized N4 control room is described in 2.11.

c) More effective unit operation due to computerized procedures

Due to computerization, the operating procedures are no longer written down on paper but are displayed on screens. These computerized procedures:

- propose action sequences rather than imposing them;
- present the actions to be taken in the form of diagrams, for use in the event-oriented approach (used for normal reactor operation); and
- present images in the form of permitted operating zones, for use in the physical state approach (used in post-accident situations).

The use of computerized procedures presents numerous advantages:

1) the difficulties of documentation management are simplified;
2) operator actions are guided because of:
   - synthetic presentation of information, enabling the operator to make informed decisions;
   - a visually clarified organization of the different operating phases;
   - a step-by-step validation of the action sequences that ensures that none is omitted and helps the operator to realize the operations that are being effected; and
   - a confirmation by the machine of the operator's choices. This provides reassurance about his decisions and enables immediately correcting any possible errors.

d) Organization of the instrumentation and control system

The above described organization of the N4 unit control room has led to arranging the overall Instrumentation and Control (I&C) system into three levels:

- level 0: the sensors and actuators,
- level 1: the automatic control devices, and
- level 2: the operating and monitoring resources.

The automatic control device level is itself organized into two parts:

Part 1 contains

- the reactor core I&C system (reactor protection system, nuclear instrumentation system, and rod control system), known as the "C03",
- the safeguard support systems I&C (diesel generators, ventilation), known as the "CS3", and
- the atmospheric steam dump I&C system, known as the "SCAP".

Part 2 contains the on/off and analog controls for the primary and secondary auxiliary systems.

High-speed data exchange takes place via local area networks.

The advantages of this organization include a large reduction in the number of electrical cables used, and the ease of modifications made possible due to standardized connections.

e) The reactor protection system (see 2.5)

The reactor is protected by the "SPIN" Integrated Digital Protection System, which:

- trips the reactor when the operating conditions so require, and
- triggers the engineered safeguard systems to counter the consequences of an accident.

The characteristics of the system structure are as follows:

- two "trains" A and B,
- fourth-order redundancy, and
- two-out-of-four logic for the control of the reactor trip circuit breakers.

1.3.4. Systems (see schematics in appendix 1).

a) Safety injection and containment spray systems (see 2.2)

The main function of the safety injection system is to ensure core cooling in the event of a break in the reactor coolant system (RCS). This system includes two identical subsystems ("trains"), each having a medium-pressure pump and a low-pressure pump. It is capable of injecting cold water into the four RCS loops simultaneously with the four accumulators connected to the cold legs.

In case of an RCS break, the containment spray system evacuates heat from the reactor containment toward the heat sink. It has two identical trains. Each of them includes a pump, a heat exchanger, and a spray ring.

These two systems are interconnected to enable, in case of total loss of one of them, long-term mutual backup of the failed system by the one still in operating condition.

b) Auxiliary feedwater system (see 2.2)

This system removes residual core heat via the steam generators during a normal reactor shutdown or in case of an accident, when the RCS is still at high pressure. It includes two independent trains that are physically separated. Each has its own electric motor-driven pump and turbine-driven pump.

In case of simultaneous loss of the normal and emergency feedwater systems, the reactor core can no longer be normally cooled. In this case, the RCS is supplied with water from the safety injection system and the resulting steam is evacuated via the pressurizer relief lines: the RCS is in a feed and bleed mode.

c) Chemical and volume control system

In normal reactor operation this system controls the volume of the reactor coolant, its chemical composition, and the core reactivity. The reactor boron and water makeup system feeds the chemical and volume control system with demineralized and degassed water with and boric acid. The chemistry of the reactor coolant system is adjusted by means of injecting additives, notably corrosion inhibitors.

d) Residual heat removal system (see 2.6)

This system removes the residual core heat, when the RCS pressure is sufficiently low, during a normal reactor shutdown or during certain accident situations. It includes two identical, independent "trains", each having its own pump and heat exchanger. The residual heat removal system is installed inside the reactor containment.

During cold shutdown, the reactor cavity and spent fuel pit cooling and treatment system is capable of taking over to remove the residual heat from the reactor core.

In the N4 design, the possibility of total loss of the residual heat removal function has been taken into account. The heat is then evacuated by a steam generator, if pressure can be built up in the RCS, or, as a last resort, by the reactor cavity and spent fuel pit cooling and treatment system.

e) Reactor cavity and spent fuel pit cooling and treatment system (see 2.6)

The principal function of this system is to evacuate the residual heat generated by the irradiated fuel assemblies stored in the spent fuel pit. It includes two pumps and two heat exchangers. The considerable thermal inertia of the spent fuel assemblies cool during repairs and maintenance.

The reactor cavity and spent fuel pit cooling and treatment system can, under certain conditions, ensure reactor cooling when the residual heat removal system is unavailable.

f) Component cooling and raw water systems (see 2.6)

The component cooling system transfers the heat from various heat exchangers and equipment units towards the heat sink via the raw water system.

It consists of two "trains", which cool the equipment belonging to systems having a safety function: - the residual heat removal system, the safety injection system, and the reactor containment spray system and a loop cooling non-safety-related equipment. Each train includes two pumps and two half heat exchangers.

1.3.5. Improving the reactor coolant system design and availability

a) The reactor vessel

The main characteristics of the N4 reactor vessel include:

- a larger diameter than that of the 1300 MWe units,
- cladding of the inner wall with two layers of stainless steel,
- manufacture of the shell rings from hollow ingots which improves the metallurgical characteristics in the vicinity of the cladding,
- a considerable reduction in the nil ductility transition reference temperature at the end of life which affords a greater safety margin with respect to the risk of brittle fracture,
- a smaller inner diameter of the reactor bottom head instrumentation penetrations, and
- an improved geometrical profile of the nozzles, which facilitates inspection of the welds and the adjacent material.

Inconel 600 is sensitive to primary water stress corrosion cracking (PWSCC) in the presence of high stresses. This was confirmed by the discovery of a leak on a Bugey 5 reactor closure head CRDM adapter. The closure head adapters for the N4 units are made of Inconel 690, whose insensitivity to PWSCC has been demonstrated.

b) Multistud tensioning machine

To improve the reactor opening and closure operations and at the same time to reduce personnel radiation exposure, Framatome has designed and manufactured a machine to tighten, tension, and loosen the studs that hold down the reactor closure head, called a multistud tensioning machine (MSTM).

c) The reactor internals

A certain number of improvements have been made to the reactor internals, based on operating experience feedback.

d) A new steam generator

One of the major improvements made in the N4 PWR unit is the new steam generator design. Some of its principal characteristics are as follows:

- a steam pressure of 72 bar, due to a new-design axial economizer;
- larger diameter manholes on the secondary side which facilitates in-service inspection and maintenance;
- tubes made of thermally treated Inconel 690 which offer greater corrosion resistance;

- an improved secondary flow design, which reduces sludge deposits on the tube sheet.

e) **A new model N24 reactor coolant pump**

The reactor coolant pump model adapted for the N4 PWR units retains certain positive characteristics of the 1300 MWe pump and incorporates some significant innovations.

f) **The N4 pressurizer and overpressure protection (see 2.2)**

The N4 unit pressurizer is equipped with an overpressure protection system which takes into account the lessons learned from the Three Mile Island accident.

This system has three relief lines. Each line is equipped with two tandem mounted valves, controlled by the pressurizer's vapor-phase pressure. The first, normally closed valve opens in case of overpressure. The second, normally open valve closes in case of depressurization of the reactor coolant system.

All three pressurizer relief lines participate in the overpressure protection function. The valves are qualified to evacuate steam, a steam and water mixture, and water alone.

1.2.6. Conceptual and analysis rules

Among the methodological improvements, the N4 safety approach includes:

- Enhancement of accident analysis include significant changes, such as long term operator's phase and loss of electrical power combination.
- A global approach concerning fire hazards: both a layout and a functional approach were implemented in the design on the basis of the RCC-I (Conceptual and Construction Rules), involving a large examination of fire induced shutdown operation.
- Finally, while keeping a largely deterministic basis for the design rules, the contribution of probabilistic safety assessments has been extensively taken into account through the feedback analysis of the PSA level 1 performed on the unit 3 of the PALUEL 1300 MW power station.

CONCLUSION

Taking benefit from significant technical innovations, methodological improvements and an operating experience feedback based upon more than 400 reactor-years of operation, the N4 reactor is and "advanced reactor". Its safety has been improved on a realistic and efficient basis without jeopardizing economics which is not the smallest challenge the nuclear industry has to face today.

2. DESCRIPTION OF 15 SPECIFIC DESIGN AREAS AS SELECTED FROM INSAG-3

In the following sections the reference to INSAG-3 is put in parentheses after each heading.

2.1. Plant process control systems (4.2.2.1)

Main control systems

The general purpose of the unit control systems are:

- to establish and maintain power equilibrium between primary and secondary systems during steady state operation,
- to constrain operational transients to preclude unit trip and re-establish steady state operation,
- to provide the operator with monitor instrumentation that indicates all required input and output control parameters of the systems and provides the operator with the capacity of assuming manual-control.

The independent parameters of the unit are:

- the control rod positions (for a given boric acid content),
- the feedwater flow,
- the turbine control valve position.

The method adopted for controlling the units is the reactor-following control: the power output is imposed by the national load dispatcher; so the turbine control valve position, the steam flow and, consequently, the thermal power are imposed (the steam pressure is free). The reactor power and the reactor coolant average temperature are adjusted by using the control rod banks. The last parameter to be controlled is the steam generator water level, which is maintained by adjusting the feedwater flow. There are eight main control systems.

Reactor control

The reactor control system enables the unit to follow load changes automatically including the acceptance of step load increases or decreases of 10% and ramp increases or decreases of 5%/min within the load range of 15% -100% P_n without reactor trip, steam dump or pressure relief.

Two automatic control modes are possible: mode A and mode X.

- In mode A the control rod position is ruled by the average coolant temperature.
- In mode X, the control rod position is ruled by the average coolant temperature and the axial offset of power.

This mode X is new and provides automatic control of the axial offset. It is expected to make load follow operation easier for the operating shift.

Pressurizer pressure control

The reactor coolant pressure is controlled by using either the heaters or the spray system within the pressurizer. The signal is the error between the measured pressurizer steam pressure and the internal value of 155 bar.

Pressurizer water level control

The water inventory of the reactor coolant is maintained by the chemical and volume control system (RCV). The error signal acts on the RCV flow control valve.

Steam generator level control

Each steam generator is equipped with a feedwater flow controller which maintains a programmed water level set point which is a function of turbine load. During normal operation, this controller regulates the full flow feedwater valve. When the load is about 15% P_n, the controller regulates the low flow feedwater valve.

Steam relief to the atmosphere

The steam relief to the atmosphere is used when the turbine by-pass system is not available and in case of:

- reactor trip,
- reactor coolant cooling.

Turbine by-pass control

The turbine by-pass system operates either when the rate of load rejection exceeds a preset value corresponding to a 10% step load decrease, or a sustained ramp load decrease, of 5%/min, or during unit startup or shutdown.

The action of this system is complementary to that of the reactor coolant temperature control by controlling the steam pressure. The signal of modulated opening of the by-pass valves is obtained by comparison between the steam and a set point determined from the load.

Turbine control

The turbine control is performed by a single controller ensuring the power control.

2.2. Automatic safety systems (4.2.2.2)

(see schematics in appendix 1)

a) **Reactor protection system** (see 2.5)

b) Primary overpressure protection system

The primary side overpressure protection system is made of three relief lines. Each line is equipped with two tandem mounted valves. Each valve is of the fluid pilot valve type. The second valve of each line, normally opened, closes in case of high depressurization, acting as an isolation valve, thus ensuring a high reliability to the primary system boundary qualified. These lines are to evacuate steam, steam-water mixture, and water alone.

c) Safety injection system

The purpose of the safety injection system is to provide water for cooling the reactor core and maintaining it under sub-critical conditions in the event of a loss of coolant accident such as:

- reactor coolant pipe break or inadvertent opening of a valve in the reactor coolant system leading to a coolant discharge which cannot be compensated by the normal makeup system,
- control rod drive mechanism break causing a rod cluster control assembly ejection accident,
- steam pipe break or inadvertent opening of a valve in the steam system,
- steam generator tube break.

This system is designed to supply the quantity of water necessary to prevent the fuel rod cladding temperature exceeding 1204°C, to ensure that the integrity of the reactor core and its geometry necessary for heat transfer are preserved. It consists of 3 subsystems:

- the accumulators: there is an accumulator connected to the cold leg of each reactor coolant loop; it is a pressure vessel partially filled with borated water and pressurized with nitrogen gas;
- the medium head injection (MHI) sub-system: 2 lines are provided with a set consisting of a pump and a booster pump. These pumps can inject water when the reactor coolant pressure falls below 110 bar;
- the low head injection (LHI) sub-system: 2 lines are provided with a pump. These pumps can inject water when the reactor coolant pressure falls below 20 bar.

The suction of the MHI and LHI pumps is connected to the refuelling water storage (PTR) tank (direct injection phase). The discharge of these pumps is connected first to all the reactor coolant loop cold legs (short term cooling) and then also to the hot legs (long term cooling).

d) Containment spray system

In the event of a loss of coolant accident or a steam pipe break, the steam from the reactor coolant as well as radioactive products are released inside the containment. The containment spray system is used to decrease the pressure and temperature of the containment atmosphere by heat removal and to remove radioactive iodine by means of a soda solution injected in the spray water.

This system is provided with 2 independent lines, each with a pump, a heat exchanger and a spray nozzle line. When the refueling water storage tank is empty, the pump suction are connected to the reactor building sumps for the recirculation phase. It is used to remove decay heat in the long-term phase.

e) **Secondary side heat removal**

Two systems are used:

- auxiliary feedwater system;
- steam relief to the atmosphere.

The auxiliary feedwater system is used:

- as a backup and emergency system for supplying feedwater to the steam generators upon loss of normal feedwater system,
- as an auxiliary system for filling the steam generators and to ensure feedwater during hot shutdown, cooldown, and startup operations.

It consists of:

- one demineralized and deaerated water storage tank; the water makeup is performed from the demineralized water storage tank through a gas stripper,
- two identical pumping sets (one for two steam generators), each of them with one motor driven-pump and one turbine driven pump in parallel. The steam for the turbines is withdrawn from the main steam lines, before the isolation valves. The components of this system are located in the fuel building.

Steam relief to the atmosphere is used in case of:

- heating up accidents (loss of offsite power, loss of main feedwater, main feedwater line break);
- transfer to RHR system in case of small break LOCA or steam line break;
- steam generator tube rupture (relief on the unaffected SG).

It consists of:

- 2 valves per SG of about 20% nominal flow rate,
- 2 separate controllers per SG, with adjustable set points.

f) **Secondary side overpresssure protection**

Each steam generator (SG) is protected against overpressure by the steam relief valves previously mentioned and by a set of seven spring loaded valves according to national regulation related to boilers, requiring two valves more than needed.

In the case of steam generator tube rupture, the faulted SG is protected against overfilling with water (coming from MHSI via the broken tube(s)) by the steam relief valves (two per SG, see above) which are qualified to evacuate both steam/ water mixture and water alone.

2.3. Protection against power transient accidents (4.2.3.1)

The following design measures are implemented to protect the reactor against reactivity induced accidents.

Functional diversity

Core reactivity is controlled under all normal operating conditions from establishment of criticality to shutdown inclusive, using two functionally diverse means. One is the control rods and the other is the variation of soluble boron concentration in the reactor coolant.

In case of accidents the negative reactivity provided by the safety injection system combined with that provided by normal reactivity control systems, is such that fuel design limits are not exceeded under incident or accident conditions leading to a reactivity increase due to excessive cooling of the reactor coolant system by the secondary system.

This negative reactivity is sufficient to ensure that core cooling capability is maintained even with the highest worth control rod blocked in the withdrawn position.

Reactivity coefficients

During operation at all power levels, Doppler and moderator feedback effects are such that the reactor is inherently stable.

The maximum and minimum limits on the corresponding coefficients will depend on several parameters (power level, initial enrichment, burnup, etc.); envelope values selected for analysis of different operating conditions are substantiated by appropriate analyses.

Reactivity variations

To preclude undesirable thermal/hydraulics conditions for fuel rod mechanical behaviour, reactivity variation meet the two following requirements:

- The maximum reactivity insertion rate is limited, whether achieved by rod withdrawal or by reactor coolant boron dilution. This is imposed due to the requirement of no fuel damage for inadvertent control rod withdrawal and inadvertent boric acid dilution.
- The maximum control rod insertion is specified for normal operation in order to limit rod worth in case of ejection and to respect the reactivity shutdown margin referred to in the following paragraph.

Reactivity shutdown margin

During all conditions of normal operation, including full power and reloading, each of the reactivity control systems is sufficient to bring the reactor to a subcritical condition under all operating conditions, including the case when the highest worth RCCA is stuck above the core.

Reactor trip

Reactor trip (free-fall insertion of all control rods into the core) is rapid enough to satisfy the limits on operating conditions.

Rod drop time is shorter than that postulated during analysis of these operating conditions.

Reloading

When reloading the reactor during refuelling or after a maintenance outage, the reactor coolant system boron concentration is sufficient to protect the core against uncontrolled boric acid dilution. This results in the requirement that the effective multiplication factor, Keff, be less than 0.95 with all control rods inserted.

2.4. Reactor core integrity (4.2.3.2)

Reactor core integrity is ensured by using an appropriate design basis and criteria for the fuel system mechanical design.

Design basis

The following requirements must be met:

a) For conditions 1 and 2

- Coolable core geometry, permitting core cooling with nominal performance, must be maintained.
- The ability to control reactivity, and in particular, to shut down the reactor must be maintained.
- Fuel assembly integrity must be ensured.

Modes of operation associated with condition 1 and 2 events shall not lead to hydrodynamic instability in the core.

b) For condition 3

- Coolable core geometry must be maintained, and in particular, effective safety injection must be ensured.
- Free-fall insertion of control rods must remain possible.
- It must be possible to shut down the reactor in spite of damage to a small fraction of the fuel rods; however this damage might preclude resumption of operation immediately after the cause of the accident has been eliminated.
- Specific fuel rod design bases are imposed for small-break LOCAs.

c) For condition 4

- Coolable core geometry must be maintained, and in particular, effective safety injection must be ensured.
- Free-fall insertion of control rods must remain possible.
- It must be possible to return the reactor to a safe state despite damaged fuel rods (major fuel damage can occur without creating severe shock waves by the dispersion of the oxide).

The requirements are fulfilled by the compliance with the following criteria.

Condition 2	0% cladding rupture DNBR > 1,3 Linear heat rate : 590 W/cm
Condition 3	Number of affected rods (DNBR) , < 5% Tclad < 1482°C without oxidation
Condition 4	Hot spot limits: Tclad < 1204°C with oxidation (< 17%) Tclad < 1482°C without oxidation Average fuel enthalpy < 225 cal/G at BOL < 200 cal/G at EOL Fuel melting < 10% Number of affected rods (DNBR) < 10%

2.5. Automatic shutdown systems (4.2.3.3)

Protection system

The objectives of the protection systems are:

- to detect any abnormal or accidental situation in the nuclear steam supply system,
- to shut down the reactor safely,
- in the event of an accident, to operate the equipment necessary to limit radiological consequences.

Reactor trip system

The reactor trip system automatically prevents operation of the reactor in an unsafe region by shutting down the reactor whenever the limits of the safe region are approached. A reactor trip can be initiated by a signal dealing with:

- the neutron flux: high flux or too fast changes,
- the reactor core protection: low DNBR (Departure from Nucleate Boiling Ratio), high enthalpy at core outlet, high quality factor for the hot channel, high linear heat rating (these physical date are continuously calculated by the SPIN microprocessors),
- the pressurizer: low pressure, high-high pressure, high level,
- the steam generators: high water level, low-low water level,
- manual trip from the control room.

During low power operation or power escalation, some trip functions are interlocked by permissive functions.

The single failure criterion applies such that no single failure occurring within the automated protection system and coincident with testing or maintenance will prevent normal initiation of protective action. This requirement affects not only system functional design, but also equipment design, layout, and operating procedures.

When a sensor is shared by the protection system and a reactor control system, redundancy shall be such that any required protective actions can be performed automatically, under the following conservative assumptions:

- failure of one sensor (initiating event),
- failure of a second sensor (single failure),
- coincident testing or maintenance affecting a redundancy level.

Accordingly, the protection system includes four independent measurement processing groups, constituting four levels of redundancy, with a 2 out of 4 voting.

Normal electric power supplies are backed up by onsite emergency power sources that comply with the requirements for independence and redundancy.

Testing equipment enables periodically checking that the Reactor Protection System is able to fulfill its function under all unit conditions for which its availability is required, without risk of spurious actuation.

Failure of the reactor trip system when challenged

By having steam generator auxiliary feedwater system startup and turbine trip actuated by a different signal from the reactor trip signal, and by using a logic system that is independent from the reactor protection system, the consequences of this failure on the first two barriers can be minimized.

The signals initiating these two actions are output by an independent logic system and diversified with respect to the reactor protection system. Consequently, the independent logic system is free from the common-mode failure that would have affected the reactor protection system in such an event. This is achieved without compromising the safety level at the plant unit (by mixing low-voltage signals, for example).

Engineered safety features actuation system

In addition to the requirements for a reactor trip for anticipated abnormal transients, adequate instrumentation and controls are provided to sense accident situations and initiate the operation of necessary engineered safety features.

The safety functions initiated by this system are:

- safety injection actuation,
- phase 1 containment isolation (after safety injection actuation),

- containment spray actuation and phase 2 containment isolation (after containment high pressure signal),
- safety injection and containment spray recirculation actuation,
- steam line isolation,
- normal feedwater line isolation,
- auxiliary feedwater system actuation,
- turbine trip.

As for the reactor trip system, some safeguard functions can be interlocked by permissive functions.

2.6. Normal heat removal (4.2.3.4)

Normal heat removal is realized by coolant circulation in the primary circuit, steam generation in the SGs, transfer of steam energy to the turbogenerator and condensation of spent steam in the turbogenerator condenser.

Scheduled sequence is proceeded in the following way:

- reactor shutdown,
- increase of boron concentration to the standby value,
- steam/water cooldown
- water-to-water cooldown at primary temperatures less than 180°C.

When the primary parameters are about 30 bar and 180°C, the Residual Heat Removal System (RHRS) can be used.

Entirely located inside the containment, the residual heat removal system is used

- to reduce the temperature of the reactor coolant to the cold shutdown temperature (less than 60°C) at a controlled rate (28°C/h maximum) during the second part of the normal unit cooldown,
- to maintain this temperature until the unit is started up again.

This system consists of 2 identical subsystems in parallel, each of them having a centrifugal pump, a heat exchanger and a cooldown rate control system.

The residual heat removal system is placed in operation after reactor shutdown, when the coolant characteristics are sufficiently low; the cooldown rate is manually controlled by regulating the reactor coolant flow through the tube side of the heat exchangers. The cold shutdown conditions are obtained approximately 20 hours after reactor shutdown.

When the residual removal system is in operation, a portion of the reactor coolant flow may be diverted to the chemical and volume control system (RCV) for cleanup purposes.

For the refuelling operation, the reactor cavity is filled with borated demineralized water by the pumps of the reactor cavity and spent fuel pit cooling system (SFPCS). After refuelling, this cavity is emptied by the residual heat removal system pumps and the water is routed to the PTR tank.

Spent fuel is stored in a spent fuel pool located in a dedicated building separated from the reactor building. This pool is cooled by the spent fuel pool cooling system (SFPCS).

Both RHRS and SFPCS are cooled by the component cooling system, used to transfer heat to the ultimate heat sink (essential service water system). These two systems consists of 2 identical subsystems, each of them having 2 pumps capable of full flow and 2 heat exchangers capable of half load.

2.7. Emergency heat removal (4.2.3.5)

In case of loss of normal residual heat removal, the auxiliary feedwater system (and the dump valves to the atmosphere) can be used.

If these systems are not available, a feed and bleed mode is used; water is supplied by the safety injection system to the primary circuit, and the safety valves on the pressurizer are operated.

When the primary circuit loses its integrity, it is a primary leakage (or break) which is dealt with as such (see 2.2).

During shutdown, while the reactor coolant system is cooled by the RHR System, the total loss of heat sink is taken into account as a beyond design event. A dedicated procedure enables cooling down the core with the secondary side if the primary circuit is closed, by steaming and by water make-up.

2.8. Reactor coolant system integrity (4.2.3.6)

Integrity of the main primary system is of importance in ensuring both plant safety and continuous reactor operation. For this reason, special emphasis is placed on the design and surveillance of the system. The corresponding measures are governed by the Order of February, 26 - 1974, applying pressure vessel regulations to the nuclear steam supply systems of water cooled reactors.

During plant operation, the reactor coolant system may be subjected to various design conditions divided into four categories, for which the resistance of the equipment to the following types of damage must be estimated:

- prevention of fast fracture,
- excessive deformation,
- plastic instability,
- elastic and elastic-plastic instability,
- progressive deformation,
- progressive crack growth.

To prevent such damage, a mechanical design code (RCC-M) approved by the French safety authority is applied.

The main primary system overpressure protection is provided by appropriate safety valves and safety actions (reactor trip) to complement normal pressure and temperature control means. Pressure is controlled by the pressurizer (using pressurizer spray or heaters) and its associated pressure relief devices and surge line, which shall be designed to absorb reactor coolant inventory changes, and to limit pressure transients due to variations in coolant loop temperature during all condition 1 and 2 events.

Pressure safety valves set to open at the system design pressure shall constitute the ultimate means of overpressure protection.

When the residual heat removal system is connected to the reactor coolant system, overpressure protection for both systems shall be provided by the residual heat removal system safety valves.

Materials of construction are chosen to satisfy various requirements, particularly to optimize the characteristics relative to the following three points:

- ability to be welded,
- corrosion resistance,
- resistance to irradiation.

The main primary system hydrotest is performed at a pressure of at least 1.25 times the highest of the design pressures of the pressure retaining components comprising the system.

The first main primary system hydrotest is performed before the first fuel loading. The second one takes place at the latest 30 months after the first fuel loading. Beyond this, the time interval between two consecutive hydrotest cannot exceed ten years.

The regulatory requirements concerning periodic testing and in-service inspection relate to:

- the access of personnel to carry out the operations required to operate remote examination devices,
- the surveillance program to check the effects of irradiation,
- the monitoring of the evolution of metallurgical indications,
- the verification and maintenance of accessories, including I&C devices.

To monitor the effects due to irradiation, specimens representative of the construction materials used in areas exposed to neutron irradiation shall be placed in the reactor internals.

To monitor the evolution of the indications revealed during the pre-service inspection, periodic inspections shall be conducted, and the recordings obtained shall be compared.

The periodicity of the corresponding inspection is as follows:

- Each time a hydrotest is conducted, an inspection of the entire reactor coolant system is carried out. The pre-service inspection which takes place at the time of the first hydrotest constitutes the reference for the following inspections.
- Additional in-service inspections are carried out with a time interval between two inspection which cannot exceed two years.

2.9. Confinement of radioactive material (4.2.3.7)

Three barriers are interposed between radioactive materials and the environment:

- the fuel matrix and the fuel cladding.
- the primary coolant pressure boundary.
- the containment.

During normal operation and most frequent incidents, the first barrier integrity is ensured by safety device actuation.

In case of loss of primary circuit integrity, the confinement of radioactive material is provided by the containment. This consists of a double wall building, the annulus between the walls being kept at a subpressure by a ventilation system. All the penetrations for pipes and electrical wires are designed to the maximum pressure and temperature that could be reached in design basis accidents.

These pressures and temperatures are kept under acceptable limits (5.5 bar) by the means of a containment spray system (CSS) able to remove the decay heat transferred to the containment through the break. The CSS is automatically actuated. Penetration isolation valves are also automatically actuated.

The safety injection system and the spray system boundary are part of the third barrier. If that part of the third barrier leaks, a dedicated ventilation system in the safeguard building prevents contamination, and liquid radioactive materials can be brought back to the reactor building by the means of re-injection lines.

2.10. Protection of confinement structure (4.2.3.8)

For the case of a severe accident leading to exceed 5.5 bars inside the containment, a special depressurization device is provided.

The atmospheric gases of the containment are discharged to the unit stack via special filters retaining most iodines and aerosols:

- 90% is kept inside the containment on a metal filter with large surface,
- the flow is then filtered by an external sand filter before release to the stack.

2.11. Monitoring of plant safety status (4.2.3.9)

The main control room (MCR) is computer based, with help of some conventional devices. This new concept of control room has been developed in the eighties with the aim of improving the man/machine interface and thus reducing the risks due to human errors.

The computerized part of the MCR, so called I&C level 2, includes four operator work positions connected to a set of computers by a dual local area network. Each work position contains three graphical CRT screens for the display of operating formats, procedures and historical data, four screens for the display of alarm information, three touch sensitive screens, a tracker ball and two functional keyboards for operator's interaction.

A wall mounted mimic panel connected to I&C level 1, easily visible from the work positions, provides the entire operating shift with an overview of the unit status.

In the case of computer unavailability, which is much unlikely because a MTBF of 10 years is specified, a conventional control panel in addition to the mimic panel enables to go to a safe shutdown state, even in the case of an accident.

The following objectives are assigned:

- reducing the amount of information presented to the operators by the means of a synthesis of information items, adequate alarm processing, and efficient diagnostic aid,
- integration of maintenance and operation actions by the means of connecting the MCR network to the maintenance computer system,
- taking into account periodic testing by automatic procedures.

Before the first implementation on the N4 units, the concept has been validated on a full scale engineering simulator. Ergonomy specialists and actual operators helped design engineers to write the specifications for the computers and the mimic panel.

The design was validated using an engineering simulator. During testing, the following observations were made:

1) the operators adapted rapidly to the computerized control stations;
2) the necessity to work sitting down, due to the concentration of displays and controls, was appreciated by the operators;
3) the wall-mounted mimic panel constitutes a link between the different operating shift members and provides a good overall view of the operating conditions of the unit, a means of monitoring their actions, and a means of fast access to essential information and immediate detection of changing situations;
4) the images displayed, along with information making them "autonomous", facilitate the work of the operators.
5) computerized alarm processing, supplying only a presentation of pertinent alarms, is appreciated.

2.12. Preservation of control capability (4.2.3.10)

The main control room (MCR) is protected against external hazards: earthquake, aircraft crash, flooding, explosion waves. It is also protected against external contamination by the ventilation systems: it can be cooled by a closed circuit system and the little amount of new air which is necessary can be filtered through iodine and aerosol filters.

In the unlikely case of MCR unavailability, for instance because of a fire, the operating shift is able to bring back the plant to a safe shutdown state using the remote shutdown station (RSS). This is located in the electrical rooms, at a level different from the MCR. The ventilation system is also different. The panels of the RSS are conventional, and are connected to the I&C level 1. Equipment of both electrical safety trains is separated. The RSS is protected against external hazards.

The RSS provides control of the following functions:

- neutron flux monitoring,
- transfer to residual heat removal system using secondary side heat removal (emergency feedwater system and steam relief to the atmosphere),
- decay heat removal using the residual heat removal system,
- automatic safety system actuation monitoring.

A full test of the operating procedure is performed during commissioning tests and a partial test is performed once per fuel cycle.

2.13. Station blackout (4.2.3.11)

Each unit on a site is connected to the grid by the means of two different lines. Within each unit the safety equipment is supplied with secured power by two diesel generator sets of 100% each. The DC power is supplied by batteries providing one hour of autarchy. A high reliability is thus reached.

Nevertheless, total station blackout is taken into account as a beyond design event. Residual heat removal is performed by the secondary side: steam relief to the atmosphere and emergency feedwater supplied by two turbine-driven pumps. A turbine-driven generator supplies power for minimum lighting, I&C and for driving a piston-pump feeding the reactor coolant pump seals. It is automatically actuated. These systems give an autarchy of at least 20 hours to the unit.

An additional generator set (gas-turbine generator) is available on each site and can be connected to any safety electrical board. Such a connection is manual and enables the operating shift to recover a power supply within a few hours.

2.14. Control of accidents within the design basis (4.2.3.12)

Any action which is necessary to mitigate a design basis accident is automatic if it is required within less than 20 minutes from the onset of the accident. These 20 minutes are thus available for system surveillance and diagnosis and for further action decisions without hurry. This initial surveillance and diagnosis, as well as further actions, are performed using a set of procedures based on a physical state approach. The diagnosis of the initiating event is not required since the actions to be done are decided at each step with consideration of the actual value of the main physical parameters of the plant.

These parameters are provided by a specific instrumentation called post accident monitoring system (PAMS). These main parameters are the following:

- water level in the reactor vessel,
- margin to saturation at the outlet of the core,
- neutron flux,
- activity concentration on the secondary side of the steam generators,
- pressure level in the containment,
- radiation level inside the containment.

Other parameters important for surveillance are displayed on operating formats and on the mimic panel, namely control rod position, containment isolation valve position, pressure and flow rates of the safeguard systems.

2.15. Mitigation and control of severe accidents

Despite the precautions taken, it is not possible to totally exclude the possibility of severe accidents extending to meltdown of the reactor core and the loss, of variable extent and delayed by variable length of time, of the radioactive substance containment function. Studies of severe accidents were from the beginning oriented towards control of the development of such accidents and mitigation of their consequences by a series of appropriate actions by making optimum use of the available resources in the installation during the accident, and by taking measures to protect the population.

The study of severe accidents of internal origin, essentially conducted on the basis of the WASH 1400 report (Rasmussen report) resulted in a distinction being drawn between three main classes of accidents, all including reactor core meltdown:

- accidents resulting in an early failure of the containment and the release, after a few hours, of the radioactive inventory of the containment without filtration (source term S1),
- accidents resulting in a delayed failure of the containment and the release, after at least 24 hours, of the radioactive inventory of the containment without filtration (source term S2),
- accidents resulting in a delayed failure of the containment and the release, after at least 24 hours, of the radioactive inventory of the containment via a filtered channel (source term S3).

The calculations of radiological consequences indicate that source term S3 is compatible with the implementation of the necessary measures - evacuation and confinement of the population - with reference to the intervention levels indicated in the International Commission for Radiological Protection (ICRP) Publication 40.

The approach followed in France has since consisted in examining the possibilities of reinforcing, by simple means, the capacity of the containment to perform its function as last barrier against the dispersal of large quantities of radioactive substances in the event of meltdown of the reactor core, without changing the basic design of the containment. To this end, "last-resort procedures" have been drawn up:

- procedure U2 is designed to detect any leakage from the containment by measurement of activity so that action can be taken to restore the containment leaktightness; it is implemented as soon as an accident situation is detected,
- the ducts in the containment basemat, provided for instrumentation necessities, have been sealed off beneath the reactor pit so as to prevent any early release of radioactive substances into the environment in the case of penetration of the basemat by "corium" (procedure U4),
- a device including a sand filter has been installed in French units to prevent failure of the containment by overpressure; this device constitutes a means of limiting the pressure in the containment to the design basis value by filtered release (procedure U5); an efficiency factor greater than 10 is obtained for

aerosols, reducing a S2 level release to a S3 level release. This device is supplemented by a prefilter located within the containment to limit onsite exposure.

With these procedures it is possible to consider source term S3, for which, on a strict health basis, adequate protection of the population can be guaranteed, as the upper bound for conceivable releases insofar at it is possible to exclude early failure of the containment (which is a large, dry, non-compartementalized double containment).

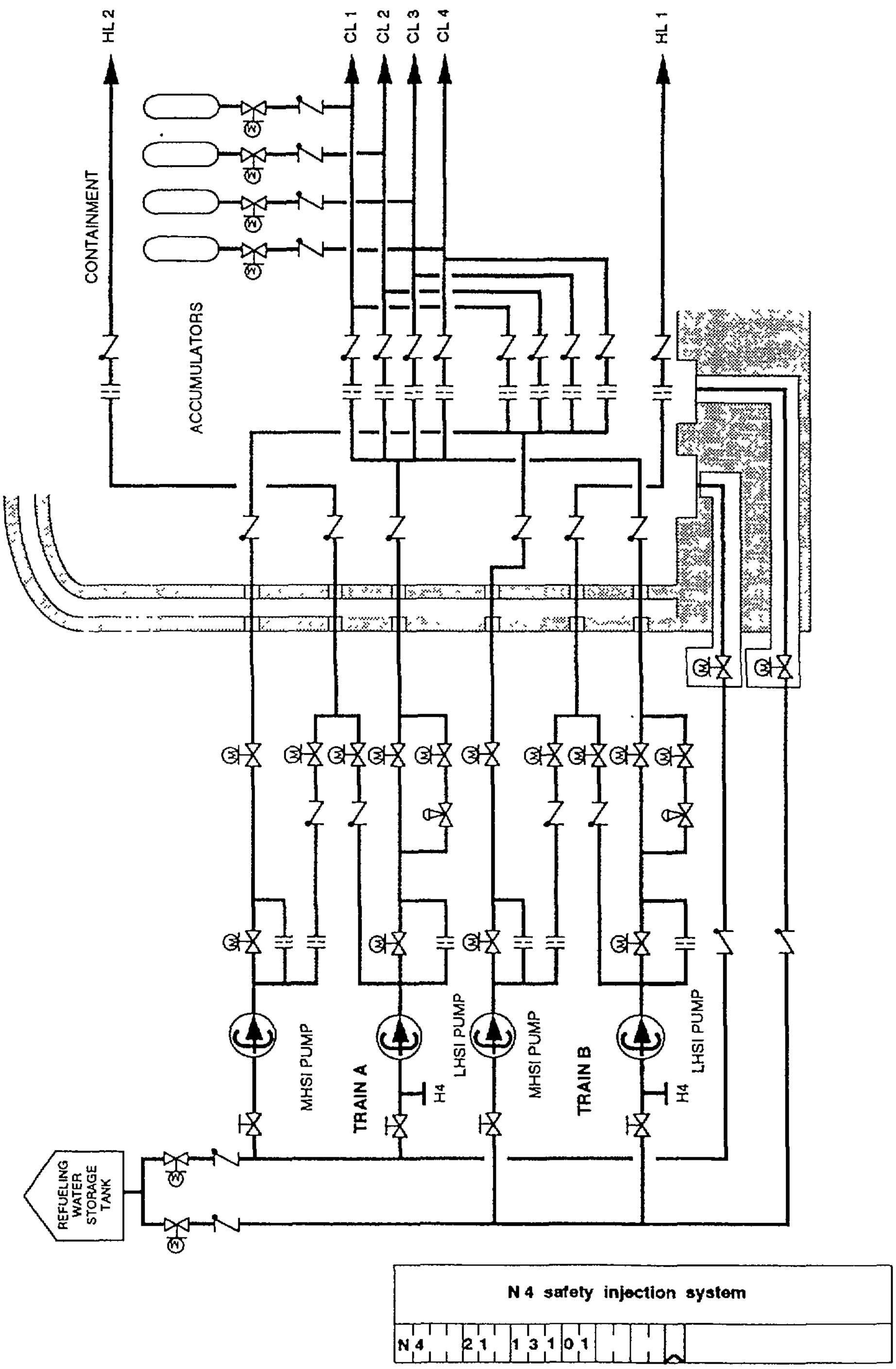


FIG. 1.

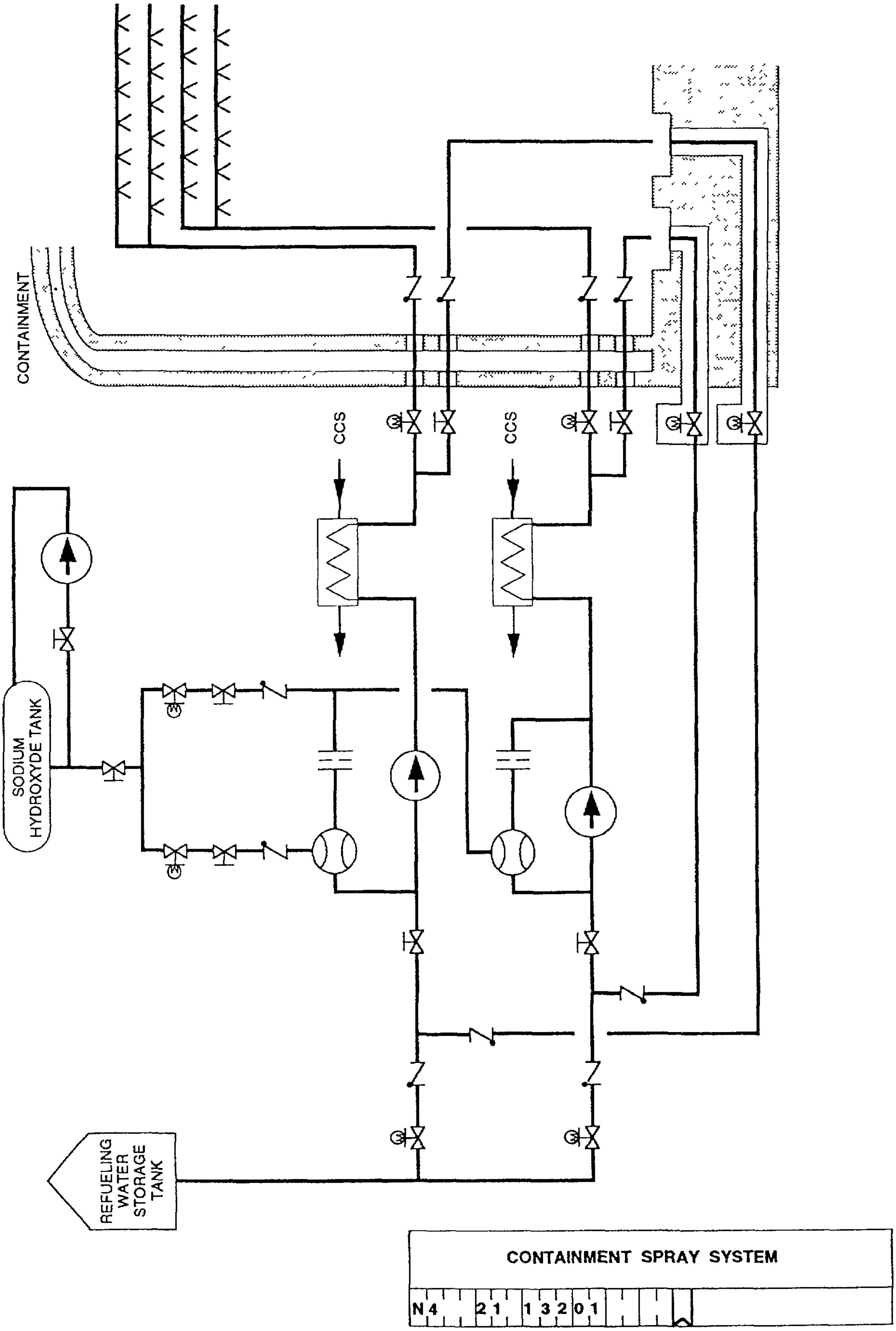

CONTAINMENT
CCS
CCS
SODIUM HYDROXYDE TANK
REFUELING WATER STORAGE TANK
CONTAINMENT SPRAY SYSTEM
N4 21 13201

FIG. 2.

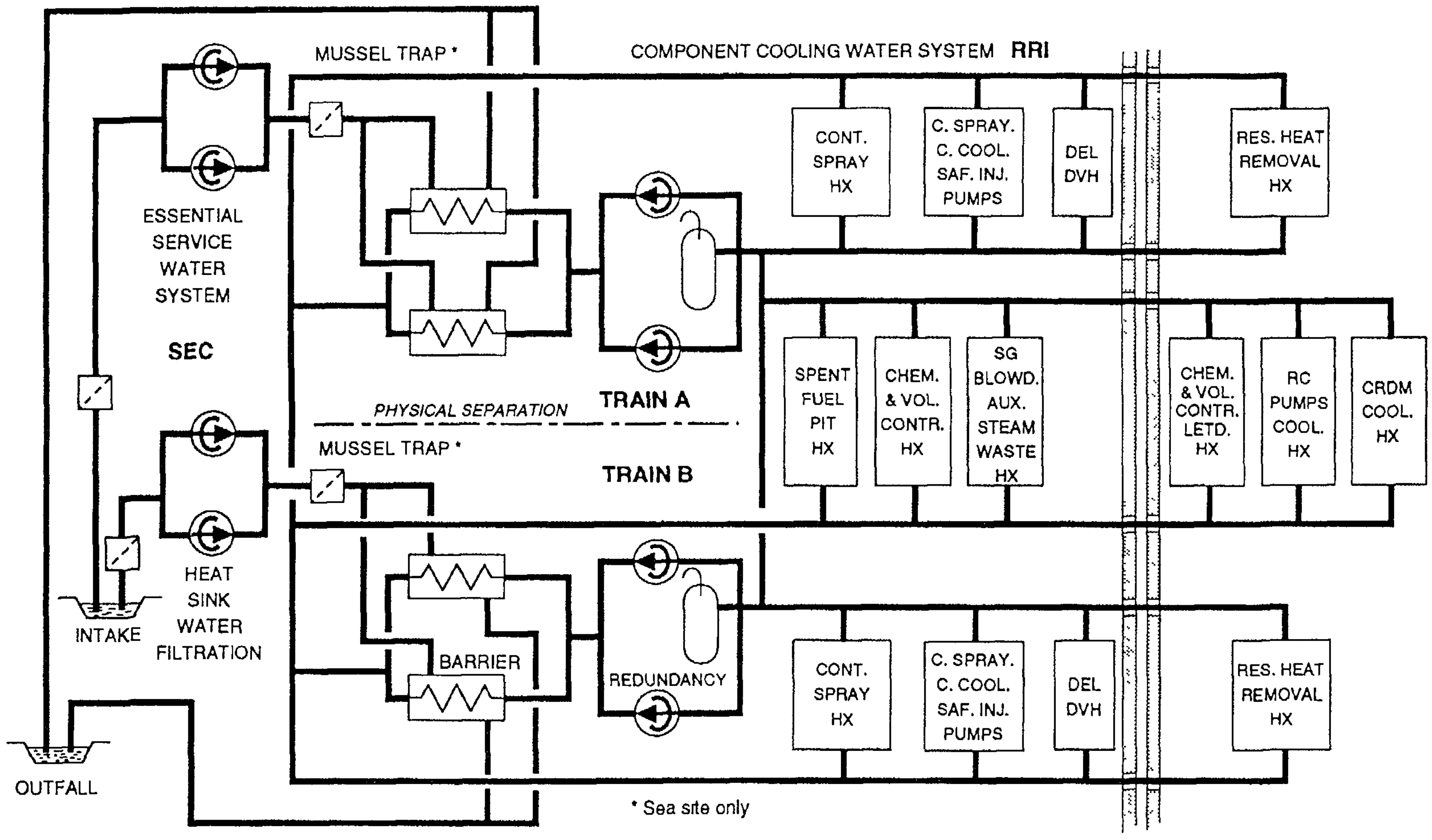
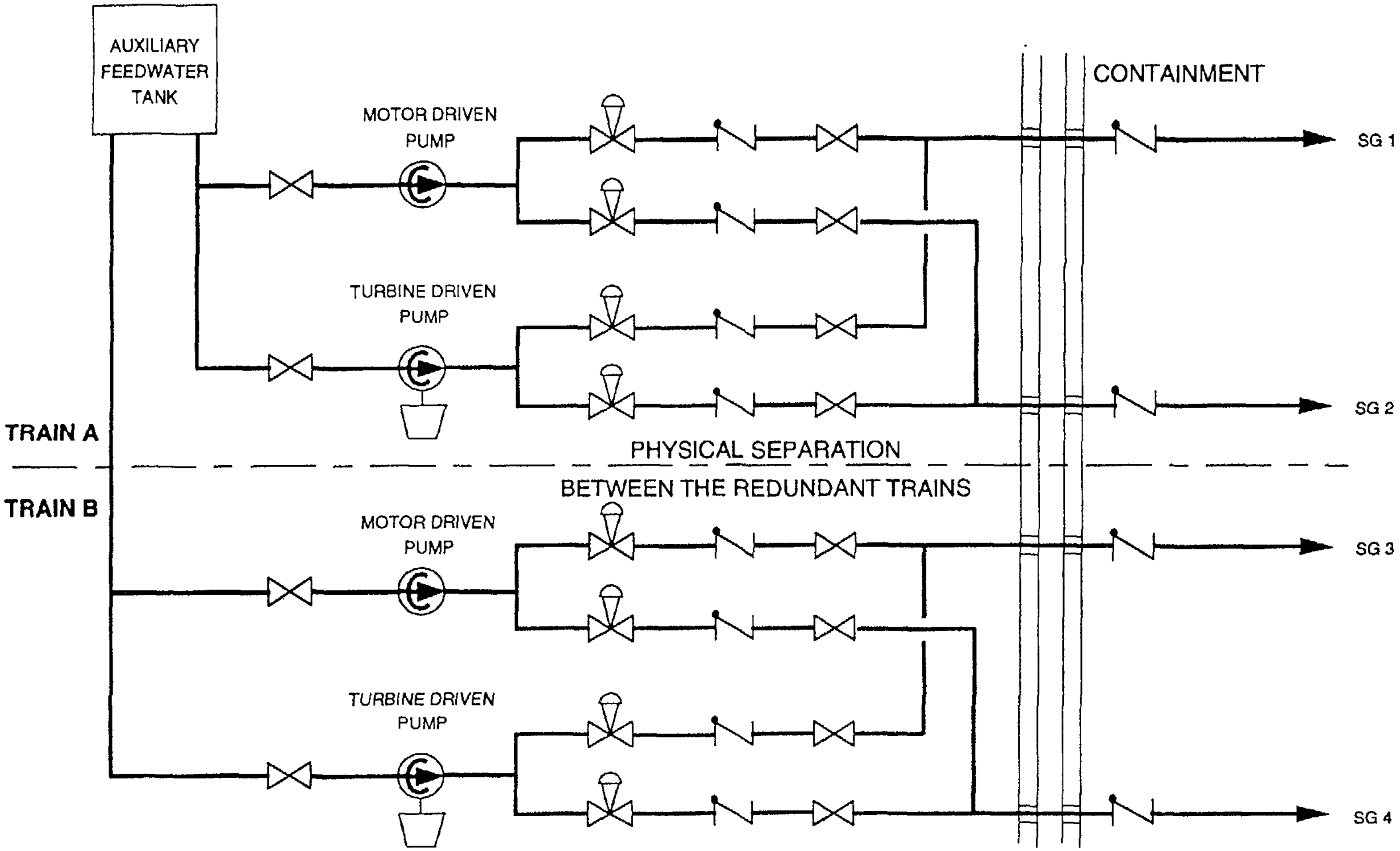


FIG. 3.

COMPONENT COOLING & ESSENTIAL SERVICE WATER SYSTEMS (*RRI - SEC*)

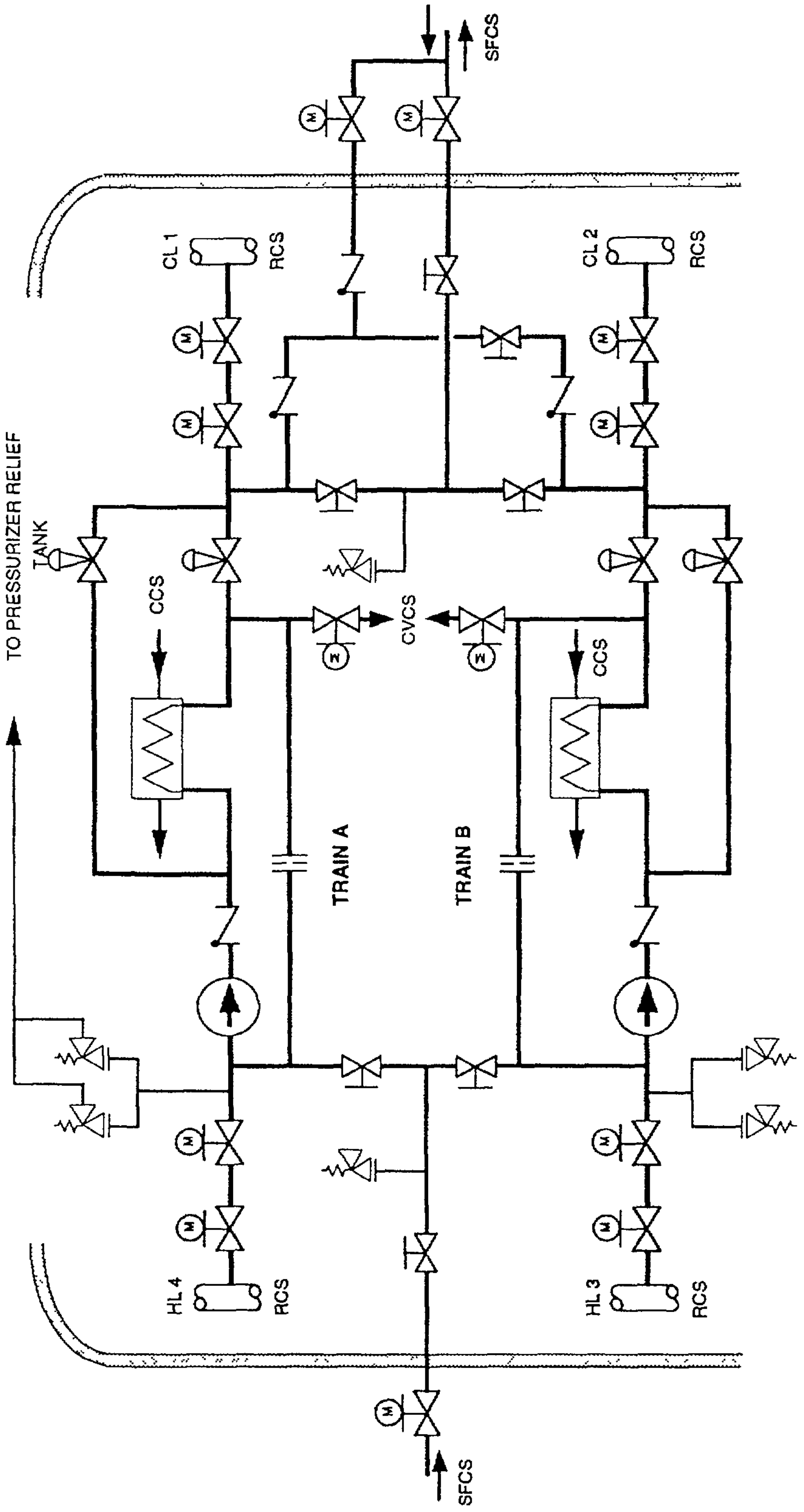
N4 21 16201



N 4 AUXILIARY FEEDWATER SYSTEM

N 4 2 1 1 3 3 0 1

FIG. 4.



RESIDUAL HEAT REMOVAL SYSTEM

N4 21 14301

FIG. 5.

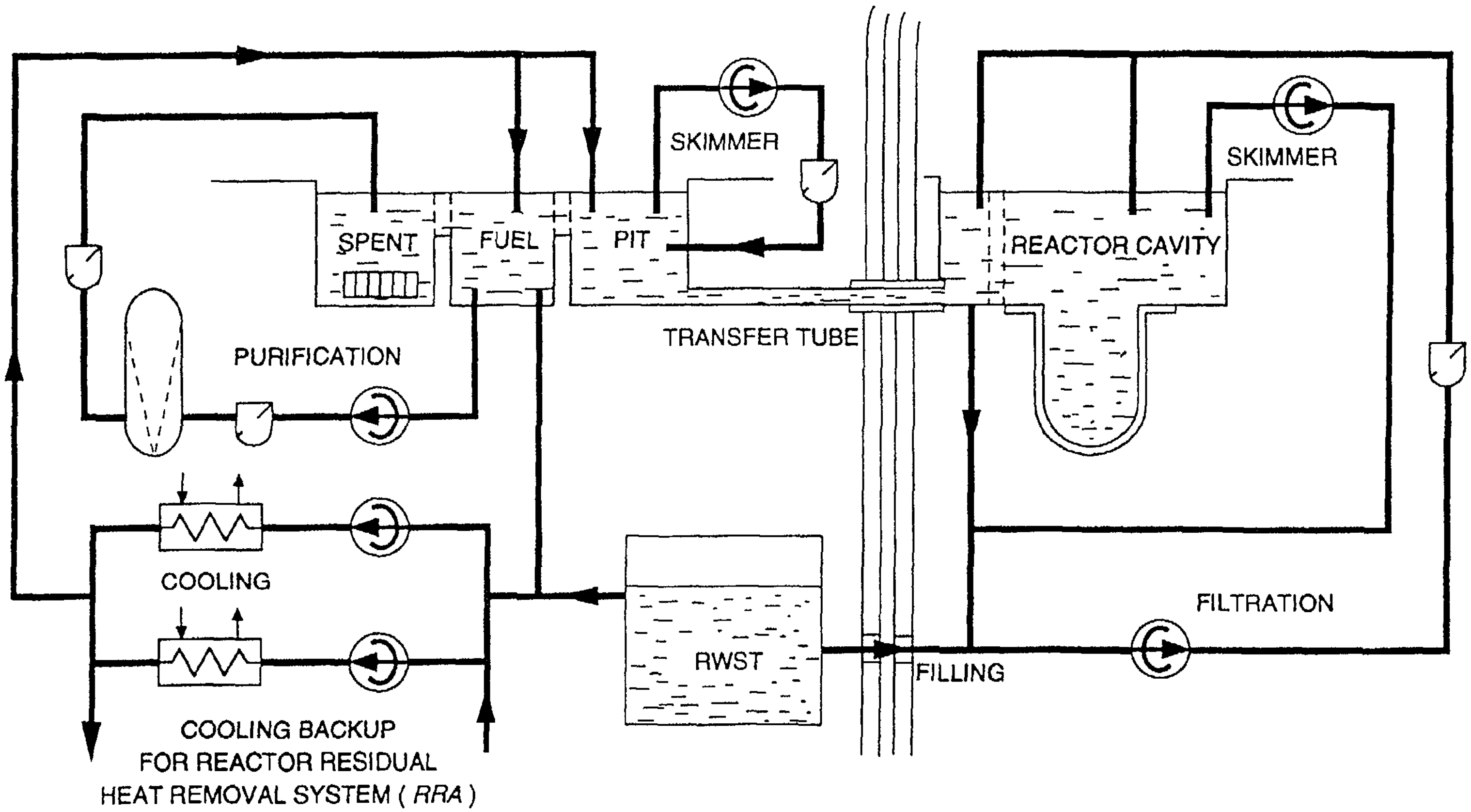


FIG. 6.

REACTOR CAVITY AND SPENT FUEL PIT COOLING AND PURIFICATION SYSTEM (*PTR*)

N4 21 16101

3. LIST OF MAIN PARAMETERS

Power

Net electrical output	1 470 MWe
Gross electrical output	1 530 MWe
Gross thermal output	4 270 MWth
Net efficiency	0.345
Turbine generator speed	1500 rpm

Containment building

Inner containment	
Type	Prestressed concrete
Inside diameter	43.80 m
Wall thickness	1.20 m
Internal volume	87 000 m3
Outer containment	
Type	Reinforced concrete
Wall thickness	0.55 m
Height at the center line	62.2 m

Reactor coolant system

Operating pressure	155 bar abs. (15.5 MPa)
Reactor vessel inlet temperature	292.2°C
Reactor vessel outlet temperature	329.6°C
Number of reactor coolant pumps	4

Reactor pressure vessel

Inside diameter	4.5 m
Total height	13.64 m
Wall thickness	225 mm
Material	16 MND5
Design pressure	172 bar abs. (17.2 MPa)
Design temperature	343°C

Steam generators

Number	4
Steam pressure at SG outlet	72.3 bar abs. (7.23 MPa)
Steam temperature at SG outlet	288°C
Steam flow at SG outlet	2160 t/h

Reactor core

Fuel material	Cylindrical U02 pellets
Core active height	4.27 m
Pellet diameter	8.2 mm
Rod outer diameter	9.5 mm
Cladding material	Zircaloy
No. of rods per fuel assembly	264
Fuel assemblies in core	205
Average linear power density	179.6 W/cm
Initial enrichment	1.8/2.4/3.1% U-235
Enrichment at equilibrium	3.4% U-235
Average fuel discharge burnup at equilibrium	39 000 MWd/tU

Reactivity control

Control rod assemblies	73
Absorber rods per assembly	24
Neutron absorber	Ag-In-Cd and/or B4C
Cladding material	SS 304
Shape	Rod cluster

REFERENCES

[1] The "White Book" for the PWR nuclear safety: general philosophy and implementation of the safety approach by EDF.

[2] INSAG-3: Basic Safety Principles of Nuclear Power Plants.

[3] N4: The 1500 MWe PWR series by Framatome.

[4] Framatome's news letter (12/93).

[[5] Safety of future reactors in France (D. QUENIART - 16/04/93).

[6] Innovative safety features of the N4 plant design (D. LANGE - Framatome; B. VIDAL-EdF), 1994.

BASIC INFORMATION ON THE DESIGN FEATURES OF THE EPR (EUROPEAN PRESSURIZED WATER REACTOR)

M. YVON, U. KRUGMANN, N. BONHOMME,
C. CAUQUELIN, G. SENGLER
Nuclear Power International (NPI),
Paris

J. P. BERGER
EdF,
Villeurbanne

France

K. SCHMIDT
Preussen Elektra,
Hannover,
Germany

Abstract

The paper describes the EPR (European Pressurized Water Reactor) power plant design of Nuclear Power International (NPI), a jointly owned company of Framatome, France and Siemens, Germany. The paper consists of three parts: - a general description of the plant concept; - a description of how the plant compares with the safety principles of INSAG-3 for 15 selected design areas; and - an extended data list. The general description outlines the main goals and objectives, the overall safety approach, and describes the major technical features of the plant. The second part discusses plant performance in the areas of: - plant process control systems; - automatic safety systems; - protection against power transient accidents; - reactor core integrity; - automatic shutdown systems; - normal heat removal; - emergency heat removal; - reactor coolant system integrity; - confinement of radioactive material; - protection of confinement structure; - monitoring of plant safety status; - preservation of control capability; - station blackout; - control of accidents within the design basis; and - mitigation and control of severe accidents. The third part, finally, presents a list of preliminary data related to the power plant as a whole, data on reactor core and fuel, on the primary and secondary side system and components, the reactor pressure vessel, steam generators, pressurizer, coolant pumps and main coolant line, and on the containment.

1. GENERAL DESCRIPTION

1.1. Main goals and objectives

The orientation chosen for the EPR follows an evolutionary approach which will achieve performance goals set at or above the highest levels reached by existing large PWRs in France and Germany. In such an evolutionary approach the large experience base of the existing plants can give confidence that these goals can be met.

In terms of cost, this means that the EPR plant target is to be competitive, in terms of total generation cost, with other electric power plants including nuclear and fossil-fired plants.

Plant availability and maintenance targets have been defined, which are reflected, e.g., in the goal to permit an average plant outage time of less than 35 days per year and a normal refuelling shutdown duration of 25 days per cycle.

Ambitious objectives have also been defined in the area of plant safety. The most visible impact on plant design stemming from these objectives are the level of redundancy and diversity in the design of plant systems and equipment, and the consideration of severe accident conditions including core melt in the plant design, leading to incorporation of core melt mitigation features.

This paper describes the overall safety approach and the major technical features. The latter are given for illustration of the present stage of the Project. They shall be considered as provisional.

1.2. Overall safety approach

The overall safety approach of the EPR follows the orientations provided in the "proposal for a common safety approach for future PWR", issued by the French Groupe Permanent Réacteurs (GPR) and the German Reaktorsicherheits-Kommission (RSK). This approach consists in deterministic bases supplemented by probabilistic analyses.

A twofold strategy is pursued compared to existing plants. First, to improve the preventive measures against accidents. Second, even if the probability of severe accident scenarios - up to core melt - has been further reduced, to implement additional features, mainly concerning the containment, to mitigate the consequences of such accidents.

This strategy is implemented by designing the plant with a strong "Deterministic Design Basis" and, beyond this basis, to consider "Risk Reduction" measures.

a) Deterministic design basis

The Deterministic Design Basis is based on systematically and deterministically chosen events.

According to their anticipated frequency, those events are categorized in 4 Plant Condition Categories (PCCs). PCC1 covers normal operation states, PCC2 to PCC4 envelop disturbed states and accidents.

The progressivity of safety and defence-in-depth principles require that for anticipated operational occurrences relatively stringent radiological limits and design criteria exist, whereas for accidents, less frequent, less stringent limits and criteria are proposed.

In the frame of safety assessment, it is shown that those radiological limits and design criteria are met, considering dedicated systems and conservative assumptions including deterministic failure assumptions in the dedicated systems.

These dedicated systems, principally safety classified, are subject to extensive efforts in order to reach a high reliability and to keep the common mode failure potential as low as possible.

The primary side safety system arrangement is described in section 1.3 b below and shown on Fig. 1.

b) Risk reduction

Nevertheless, it is intended to consider, beyond the Deterministic Design Basis, events with multiple failures and coincident occurrences up to the total loss of safety-grade systems on a probabilistic basis in order to limit the residual risk. Severe accident design release limits have been specified which are chosen in such a way that no stringent offsite emergency response actions (such as evacuation or resettlement) are necessary outside the immediate plant vicinity.

Two safety objectives have been set up (including all events and all reactor states)

- probability of core melt $< 10^{-5}$/reactor x year,
- probability of large releases $< 10^{-6}$/reactor x year.

Based on these objectives, more specific and practical probabilistic design targets for use during the early design phases of the project have been defined as follows:

1) The integral Core Melt Frequency (CMF) shall be 10^{-6} per reactor and year for internal events from power operation.
2) Shut-down states shall contribute to the integral CMF for internal events less than power states.
3) The integral CMF (internal events) associated with early loss of containment shall be 10^{-7} per reactor and year.

Two Risk Reduction Categories are introduced, and representative scenarios have been defined for both, core melt prevention (i.e. Risk Reduction Category A - RRCA) and large releases prevention (i.e. Risk Reduction Category B - RRCB), in order to provide a design basis for risk reduction features.

Those risk reduction features include, e.g.:

- primary system discharge into the in-containment refuelling water storage tank in case of total loss of secondary side cooling (RRCA),
- features for corium spreading and cooling, for hydrogen recombination, and for containment heat removal in case of severe accidents (RRCB).

The safety assessment of RRCA is performed in the form of a level 1 PSA. The safety assessment of RRCB is intended to be largely deterministic, because reliable level 2 PSA will only be possible at the end of the EPR design. In any case, the assumptions and design criteria in the risk reduction area will be as realistic as possible.

c) External and internal hazards

External and internal hazards are not directly assigned to the various plant condition categories or risk reduction categories, in order to avoid the study of numerous sequences. But the main principles behind the deterministic design basis and the risk reduction approach (namely: the more conservative or more realistic assumptions and the different acceptance

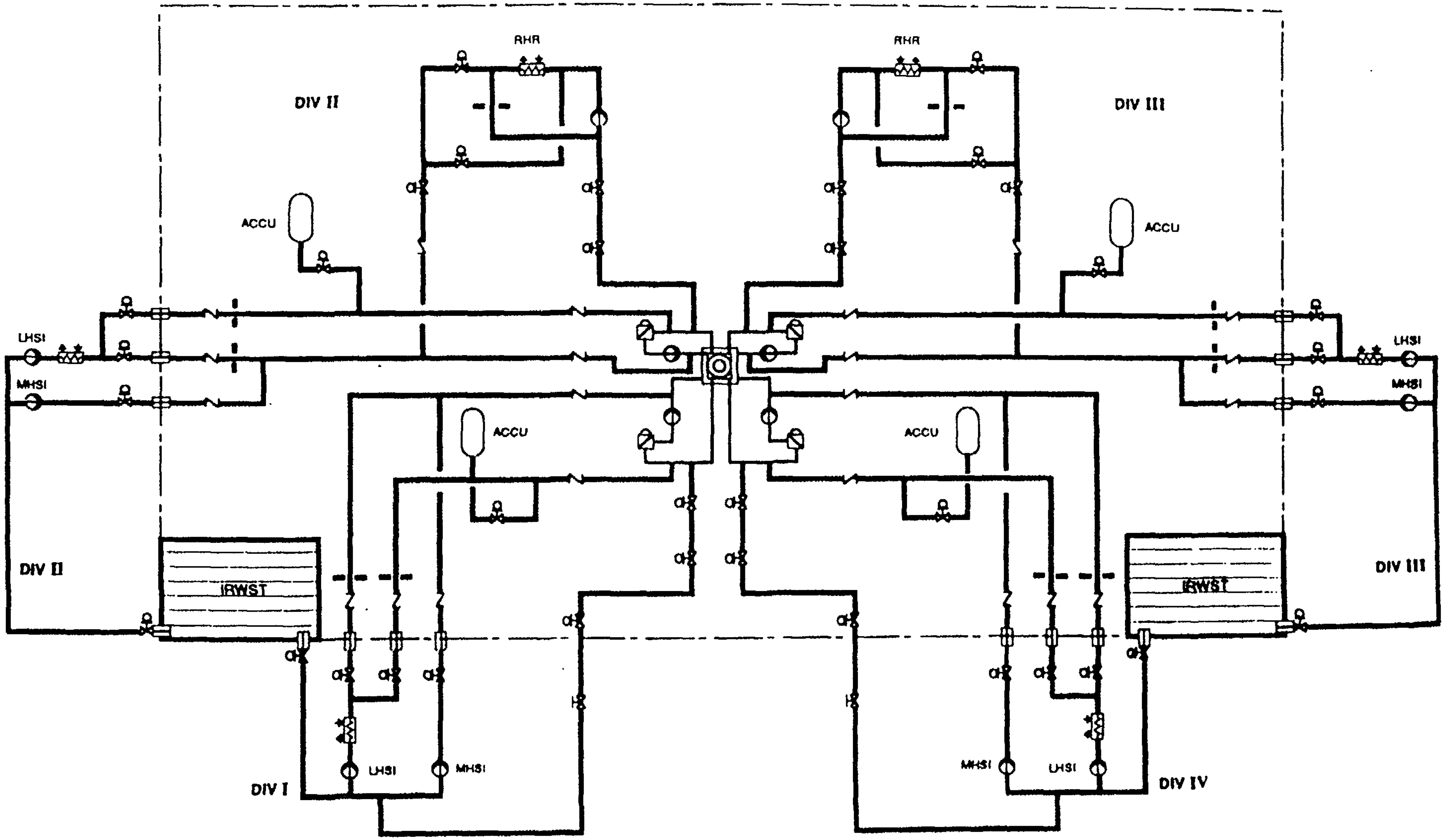


Fig. 1 - Primary side safety systems

criteria, especially the radiological limits for the different event categories) are also applied accordingly for dealing with external and internal hazards.

Natural or man-made external hazards are site-dependent. For the design of the EPR the boundary conditions are chosen in such a way, that it should be possible to construct the Nuclear Island on potential sites in France and Germany, however not enveloping all French and German sites. Sites with an extreme external hazard potential (e.g. direct vicinity to a chemical plant, or to a big airport, high seismicity areas) are not taken into consideration as potential sites. In order to be able to construct the EPR outside France or Germany in higher seismicity regions, the design shall be adaptable to higher earthquakes than the design earthquake without major layout changes.

- **Earthquake**

The USNRC Regulatory Guide 1.60 spectrum, scaled to 0.25g, will be assumed at the free field level for each horizontal component, independently of the soil conditions. It is foreseen to use later on a spectrum better adapted to the specificities of the Western Europe seismic conditions.

- **Aircraft crash**

Allowance for aircraft crash is based on a probabilistic risk assessment, as the statistical data are sufficiently representative and the possible events are sufficiently well known.

General and military aviation crashes are taken into account for plant design. A design load case was defined on the basis of a military aircraft crash of the following characteristics:

- mass : 14 tonnes
- velocity : 180 m/s
- impact area : 7m^2

- **Explosion pressure wave**

The probability data concerning the risk of aggression by an external explosion for various sites indicate that they are closely related to the industrial environment of each site and therefore to the localization chosen for the site.

For the EPR, the design is based on an incoming pressure wave with a maximum overpressure of 100 mbar. The level of protection will be verified and possibly modified on a site by site basis.

- **Internal hazards**

The internal hazards loads (e.g. fire loads, missile loads, jet impingement loads, flooding level loads) are design dependent. In the early state of the conceptual phase of the EPR development, it is not possible and necessary to quantify these loads. The main concern in this early design stage is to define the overall plant layout in such a way that these loads are minimized and that an easy protection of sensitive equipment is achieved, preferably by physical separation or by provision of strong civil structures, e.g. separating the redundancies.

Nevertheless, should an internal hazard occur in one division, the consequences will be limited to this division. Necessary interdivisional connections are minimized and protected against spreading of hazard consequences assuming a single failure.

In conclusion the protection against external and internal hazards includes the divisional separation of safety-grade systems and the physical protection of the containment including the reactor coolant pressure boundary. By this means it is achieved that the risk of inadmissible releases or common-mode-failures of safety-grade systems is consistent with the deterministic design basis and the probabilistic targets of the EPR.

The building arrangement is described in section 1.3d below and shown in Figures 2, 3 and 4.

d) Severe accident approach

As already stated above, an important innovation of the EPR project is the explicit and comprehensive consideration of severe accidents at the design stage.

The overall approach to limit the external radioactive releases in a severe accident sequence is aimed at:

- avoidance of early containment failure or by-pass,
- cooling of the corium in the containment and retention of remaining fission products by water covering,
- preservation of the containment functions, reliable isolation of the containment on demand, low leakage towards the environment, prevention of the basemat meltthrough, ultimate pressure resistance to cope with energetic events,
- pressure reduction of the containment by means of heat removal,
- collection of unavoidable leakages into the atmosphere of the annulus and release to the stack after filtration.

The investigations concerning core meltdown accidents are based on findings of national and international reactor safety research projects. Various accident sequences are considered that could lead to core meltdown. They can be classified as follows, taking into account the potential status of the containment :

1) Sequences leading to a core melt with the primary system at low pressure. It is assumed that a core meltdown at low pressure could occur, for example, after failure of the emergency core cooling systems in the case of a loss-of-coolant accident caused by a large break of a reactor coolant line. The steam escaping through the leak into the containment causes a rapid pressure relief in the Reactor Coolant System (RCS). If the core is not cooled, melting at low pressure could happen.
2) Sequences leading to a core melt with the primary system at high pressure. It is assumed that a core meltdown at high pressure could occur if, following a transient or a loss-of-coolant accident through a small leak, heat removal becomes inefficient or failes entirely for a longer period of time. The Reactor Coolant System (RCS) would remain under high pressure and thus the RPV could fail due to steel ablation by the molten corium.

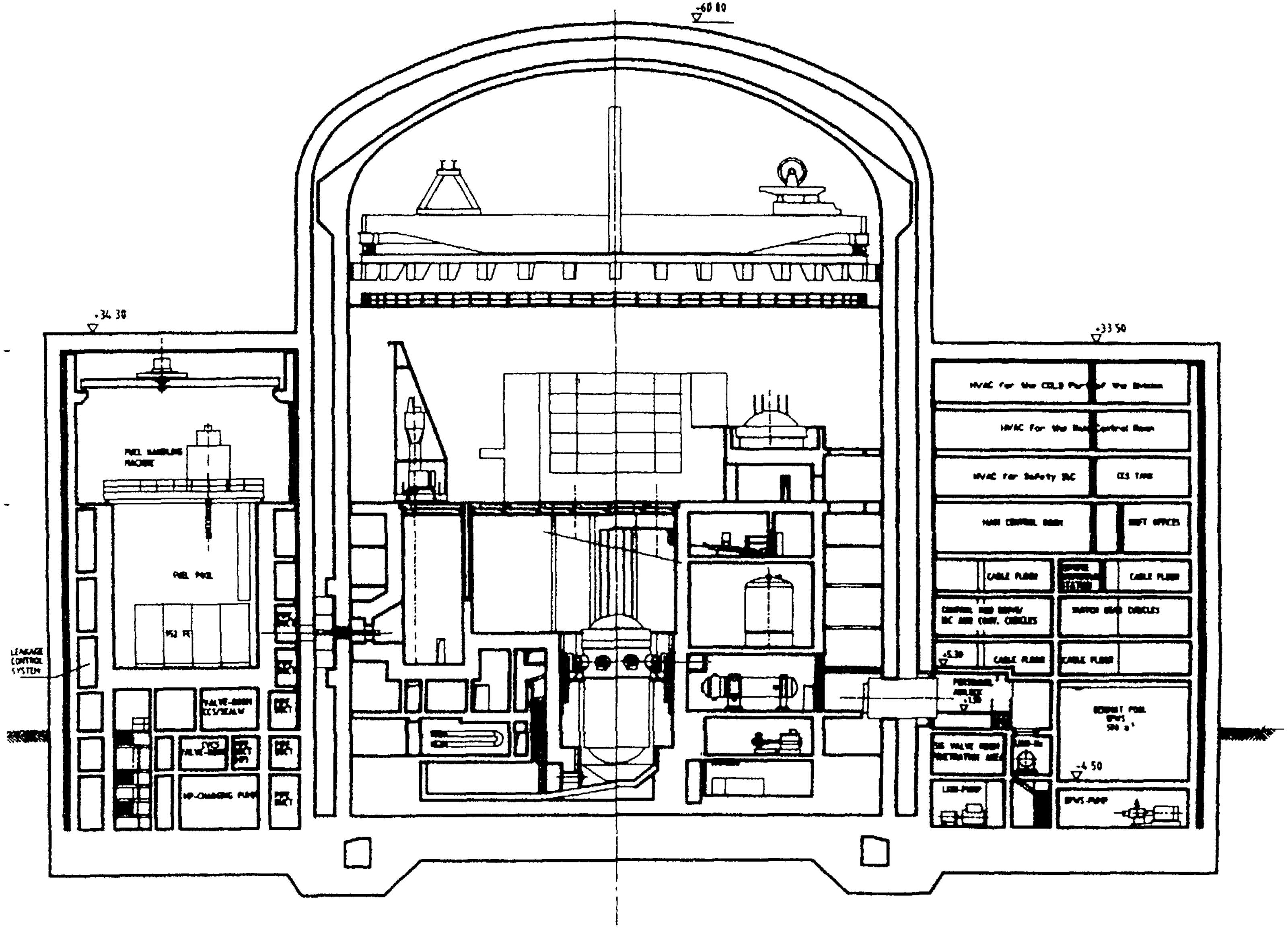


Fig. 2 - Building Arrangement - Section A-A

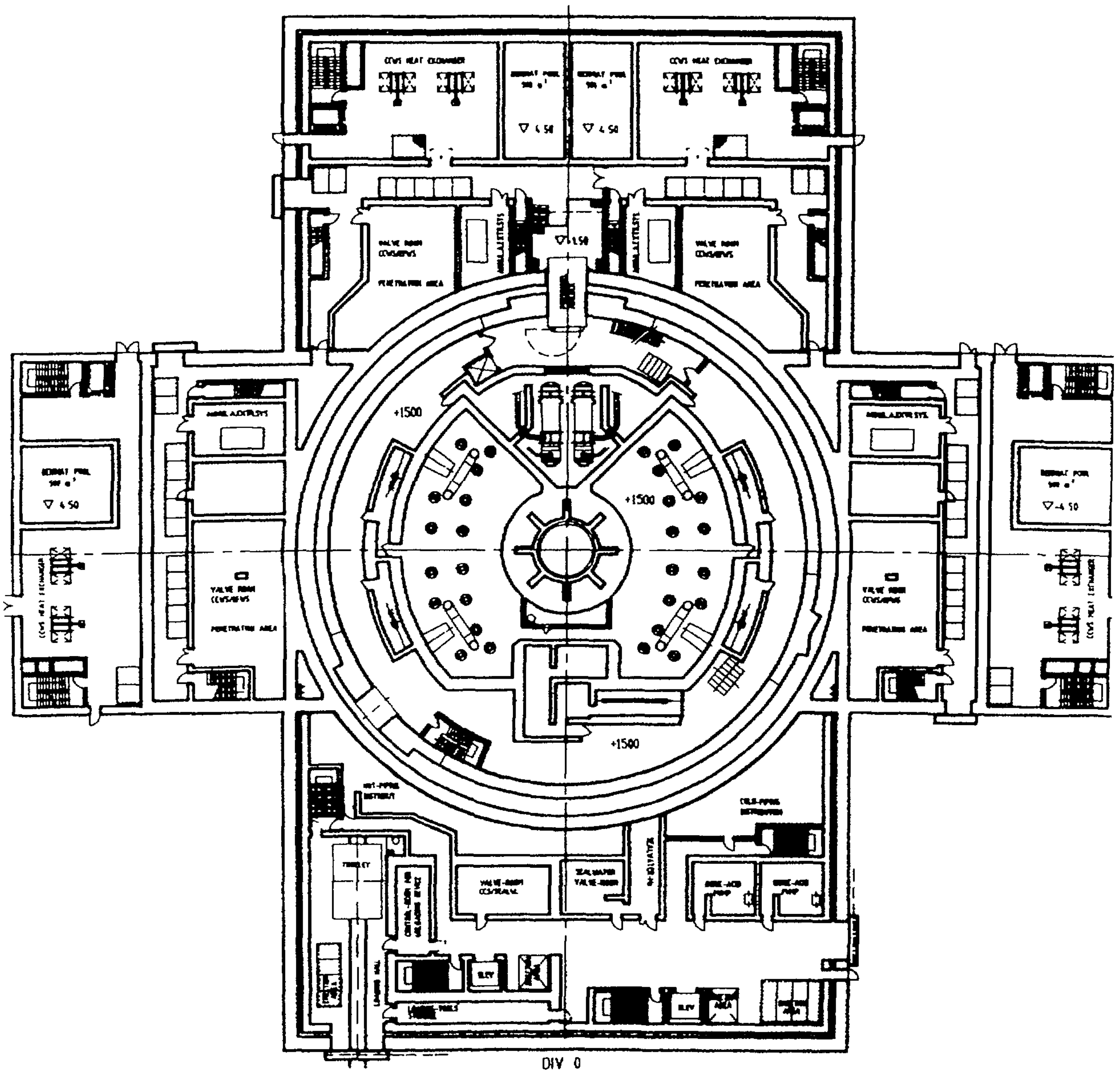


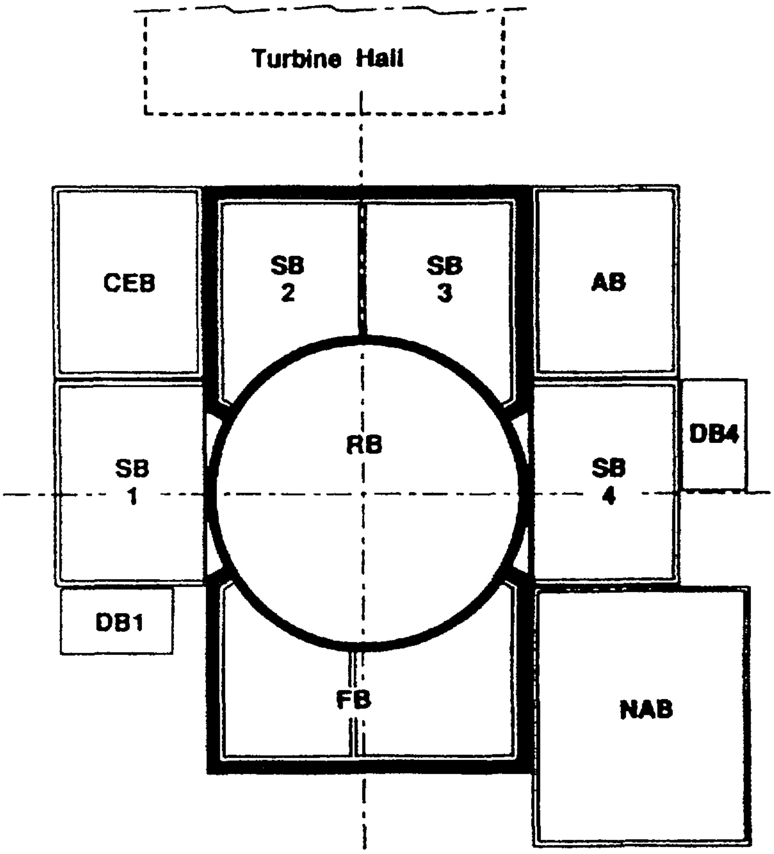
Fig. 3 - Building Arrangement - Plan view - 8,60m

3) Sequences causing a severe core damage and a containment bypass (e.g. failure of a steam generator tube or of a system connected to the primary system and routed outside of the containment).

4) Sequences with severe core damage and an independent containment loss or pre-existing leaks (e.g. "open" containment during refuelling period).

The sequences of type 1 are considered for the third barrier design and will be discussed more extensively below.

The sequences of type 2 will be reduced to such low probability that their consequences need not be considered in the definition of containment design loads. This can be achieved by provision of specific means for prevention of the high pressure core melt scenarios. The accident sequences with a high RCS pressure can be transferred with special depressurization measures to conditions under low pressure before RPV failure.



SB : Safeguard Building
AB : Access Building
CEB : Conventional Electrical Building
RB : Reactor Building
FB : Fuel Building
NAB : Nuclear Auxiliary Building
DB : Diesel Building (DB2 and 3: location under investigation)
▬ : Airplane crash protection

Fig. 4 - Plot Plan

Similarly, the sequences of type 3 and type 4 will be addressed in the EPR design, and in particular in the design of containment isolation provisions and in the main and auxiliary fluid systems design, e.g. those foreseen for mitigation of Steam Generator Tube Rupture accident scenarios. Evaluation of these sequences is important to ensure an adequate level of reliability of containment isolation and prevention of all possibility of containment by-pass, but they are not those leading to the most severe structural design loads for the containment. As regards the type 4 sequences, specific attention is paid to the possible accident scenarios during shutdown and refuelling conditions.

The main practical consequences of this approach are described in the chapter 1.3.

e) Other principles

For the EPR design, other principles were applied in order to improve the prevention of the severe accidents. Those principles are:

- simplification and diversification of safety systems aiming at improving operational safety and reducing the effects of failures,

- systematic physical separation of safety systems which limits the consequences of failure-initiating events,
- using of passive features if, and only if, they really improve the reliability of the function they perform,
- increased grace periods for operator actions,
- and improved man-machine interface.

1.3. Major technical features

As noted above, the conceptual design and harmonization effort of the past years has allowed definition of the main features of the EPR plant. In some aspect the features are preliminary and may evolve during the upcoming Basic Design phase.

a) *Essential design and operating data*

The EPR product is a nuclear island for a large, evolutionary plant, of 1400/1500 MWe power rating. The reactor is designed to allow optimization of the fuel cycle to meet the future utility needs: high burnup (up to 55-60 GWd/t), possibility of plutonium recycling, extended fuel cycle lengths. The main reactor core and reactor coolant system operating data are listed in chapter 3.

Principal reactor coolant system components are enlarged relative to existing practice: a larger reactor pressure vessel will accommodate the large core size. Pressurizer and steam generator (secondary side) are enlarged to improve plant transient response. The Reactor Coolant Pump (RCP) characteristics will, however, be maintained in a range compatible with existing RCP designs so that no important new RCP development is needed.

b) *Safety systems configuration*

Important safety systems and their support functions (safety injection, emergency feedwater, component cooling, emergency electric power) are arranged in a four train configuration. The layout comprise four separate divisions, corresponding to the four trains (see figure 1). A simple and straightforward system design approach is favoured, thus facilitating operator understanding of plant response and minimizing configuration changes.

The Safety Injection System features an In-containment Refuelling Water Storage Tank (IRWST), and is based on injection in both hot and cold legs of the RCS, thus avoiding re-alignment for recirculation and injection to hot legs in the long term phase. Together with a heat exchanger in the low-head injection (LHSI) flow path, this concept ensures emergency core cooling without the need of a containment spray system for design basis accidents (a spray system of reduced size is provided for containment cooling in case of severe accidents, see below).

The primary side safety systems are designed with stringent acceptance criteria such that the systems be able of ensuring limited core damages, even in case of large breaks. The delivery head of the medium head safety injection system will be adjusted below the steam generator relief and safety valve set points. In case of a steam generator tube rupture, and after the initial transient, the affected steam generator will be isolated and the primary and secondary pressure will equalize in this steam generator thus limiting to negligible levels the radiological releases following such accidents.

A separate Residual Heat Removal System is provided, arranged in two trains and installed inside containment to minimize risk of containment bypass. Adequate additional redundancy/diversity in decay heat removal is ensured by two of the four LHSI trains, which can serve in RHR mode at low RCS temperature.

The prevention of high pressure core melt scenarios implies a high level of reliability for the secondary side heat removal system. This is an important aspect of the EPR design. Detailed investigations, in terms of reliability as well as of operation and cost, were carried out to compare active and passive systems: either an active emergency feedwater system with diversified power supply of the pumps to achieve a very high reliability, or a passive-type secondary side cooling system operating in a closed loop. On the basis of the performed assessments, the active emergency feedwater system has been selected to be used for the EPR. It is composed of four separate and independent trains, each with an emergency feed-water pump supplying feedwater to one of the four steam generators.

By this system organization, the principle of simplification is fulfilled, as well as the principle of diversification. As a matter of fact, any safety-grade system function can be ensured by another system (or group of systems), as summarized in figure 5.

c) Severe accident features

As introduced in the preceding chapter 1.2, the EPR strategy includes both preventive measures aiming at practically eliminating the corresponding accident situations and mitigating features aiming at limiting the releases within the prescribed limits.

Safety-grade system function	Complementary system function					
MHSI Medium head safety Injection system	Fast secondary-side presure relief	+	Accumulator Injection system	+	LHSI Low heat safety Injection system	
LHSI Low head safety Injection system	MHSI Medium head safety Injection system	+	RHR Residual Heat Removal System	or	Secondary-side Heat removal system	(for small breaks).
RHR Residual heat removal system	Secondary-side heat removal system	or	LHSI Low head safety			
Fuel pool cooling system	Fuel pool heat-up (bolling)	+	Coolant fill up			
Secondary-side heat removal system	Primary-side bleed and feed					

Fig. 5 - Diversification of safety systems

Consequently, the EPR design includes:

- The prevention of high pressure core melt situations, firstly by a high reliability of the decay heat removal systems, complemented by depressurization means (pressurizer relief valves). This depressurization at the same time eliminates the danger of direct containment heating. The consequences of an instantaneous break of the RPV with full cross section at a pressure of about 20 bar are nevertheless taken into account for the layout.

- The prevention of hydrogen combustion with high loads (high turbulent global deflagration/DDT/detonation) by reducing the hydrogen-concentration in the containment at an early stage by catalytic H_2-recombiners and, if necessary, by selectively arranged igniters. The prevention of molten core-concrete interaction contributes in reducing the amount of hydrogen generated. The potential effects resulting from the deflagration phenomena are considered in the design of the containment and of the internal structures.

- The prevention of ex-vessel steam explosion endangering the containment integrity by minimizing the amount of water where the corium is spread.

- The prevention of the molten core-concrete interaction by spreading the corium in a dedicated spreading chamber. This original EPR feature consists of a large area (about 150 m^2) outside the reactor pit. The reactor pit and the spreading compartment are connected via a melt discharge channel which has a slope to the spreading area and is closed by a steel plate (see figure 6). This steel plate (possibly covered with refractory material) resists melt through for a certain time in order to accumulate the melt in the pit. The spreading compartment is connected with the In-Containment Refuelling Water Storage Tank (IRWST) with pipes for water flooding after spreading; these pipes are closed during normal operation and accident conditions by plugs which will be molten by the corium after spreading. The limitation of the containment pressure increase by a dedicated containment heat removal system which consists of a spray system, with a possibility, in the long term, to subcool the water and therefore to decrease the containment pressure down to the atmospheric pressure.

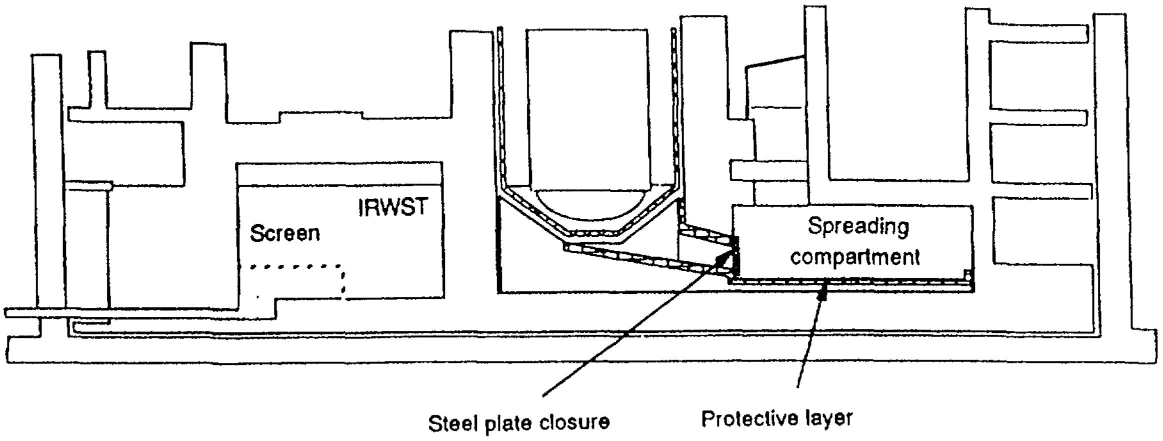


Fig. 6 - Corium Spreading Concept

- Even if all other systems are unavailable, the containment design pressure (~7.5 bar) grants a grace period of about 12 to 24 hours after the accident before having the necessity to use the spray system.

- The collection of all leaks, preventing any bypass of the confinement. This is achieved by a double wall containment (see figure 2). The leaks which might escape from the inner wall are therefore collected in the annular space, where a subpressure is maintained, and which is vented to the stack via an appropriate filter. All systems in connection with the containment atmosphere or the RCS are made leaktight. In addition, air locks and ventilation valves are equipped with a leak collection system. Finally, all penetrations (except the main steam and feedwater lines) being directed to the surrounding buildings, an efficient retention of all possible residual leaks can be ensured.

d) Containment and general layout

A review of possible options of containment technology has resulted in the adoption of a double concrete containment design for the EPR. The particular design concept favoured the use, for the inner containment wall, of the same prestressed concrete technology as currently in use in the four-loop 1300 and 1450 MWe plants in France. The leaktightness requirement of less than 1% volume can be ensured without provision of a containment liner. A secondary wall, in reinforced concrete, is provided to complete the double containment arrangement. In this way the EPR project will take benefit of the experience and operation of the existing plants.

The severe accident conditions described in the previous sections lead to more severe design conditions compared to the existing French plants, and will thus result in an extrapolation of the design parameters. In this respect, the most important factor is the increased design pressure, which has been defined as 7.5 bar abs.

The prestressed concrete inner wall, with design pressure at 7.5 bar abs, will also ensure capability to perform an integral leakrate pressure test in air at 7.5 bar, thus providing positive proof of containment structural and leaktightness capability for the entire range of pressures of all severe accident scenarios.

In terms of general layout (figures 2 and 3), the organisation of the safety systems in four totally separate trains leads to the location of each train in a specific area or "division" in such a way that it is protected against propagation of internal hazards like fire, high energy line break, or flood occurring in any other train. To reduce the length of their connections to the reactor coolant system, the trains are radially distributed like the primary loops to which they are individually assigned.

One train of the safety injection system and of the emergency feedwater system is installed in each of the four safeguard buildings. The fluid systems are located in the lower part of the buildings. In the upper part, there are the electrical and I&C equipment inclusive the main control room and the remote shutdown station.

The spent fuel pool and new fuel storage with associated equipment for handling and transfer are housed in the so-called fuel building which also houses the chemical and volume control system.

The reactor building, the safeguard and the fuel buildings are designed to withstand earthquakes and pressure waves due to explosions. These buildings rest on a common raft. Water tanks, primary system equipment and other heavy loads are, as far as possible, located at low elevations.

The protection against aircraft crash is achieved with the EPR design (figure 5) by:

- the strength of the outer wall of the reactor building containment,
- the reinforced concrete shell covering safeguard buildings 2 and 3 and the fuel building (potentially induced vibrations in case of external hazard are minimized through decoupling of the inner building structures from the protective shell),
- the geographical separation of safeguard buildings 1 and 4, considering potential destruction of only one division under the assumed circumstances.

The main control room and the remote shutdown station are located in the "bunkered" safeguard buildings 2 and 3 to remain operable in case of aircraft crash. In the safeguard buildings 1 and 4 lower parts, local reinforcement of the civil structures protect the safety injection system to avoid drainage of the IRWST under accidental circumstances.

e) *Man-machine interface and I&C systems*

Due consideration is given to the human factor at the EPR design stage, taking into account aspects of operation, testing and maintenance. The general aim is to minimize the possibilities for operator errors. This is achieved by applying appropriate ergonomic design principles and by providing sufficiently long grace periods for the operator responses. The necessary length depends on the complexity of the situation to be diagnosed and on the actions to be taken.

As a deterministic design basis, a grace period for control room actions of 30 min is used, and of 1 h for local actions. For potential risk reduction measures the use of portable equipment is assumed within 6 h, and the use of heavy additional equipment within 3 days.

Sufficient and appropriate information is made available to the operator for a clear understanding of the plant status, including severe accident conditions, and/or the clear assessment of the effects of his interventions. Emphasis is placed on the use of computer techniques for reliable diagnostics systems for operator support.

The man-machine interface concept for process and accident control respects the properties and abilities of the operator and brings the capabilities of I&C for operational and safety tasks in an optimum way into action without overloading the operator.

The failure assumptions for the design of the I&C systems are based on the overall safety criteria for system design and on the functional requirements on the fluid systems. It requires independent I&C sub-systems assuring that the total loss of one sub-system will not influence the remaining I&C.

The proposed I&C systems are based on equipment relying on digital technology using preferably "off the shelf" electronic components. Their functional requirements including the resulting failure models are dependent on the functional requirements of the fuild systems.

2. DESCRIPTION OF 15 SPECIFIC DESIGN AREAS AS SELECTED FROM INSAG-3

In the following sections the reference to INSAG-3 is put in parentheses after each heading.

2.1. Plant process control systems (4.2.2.1)

Principle: *Normal operation and anticipated operational occurrences are controlled so that plant and systems variables remain within their operating ranges. This reduces the frequency of demands of the safety systems.*

The EPR is designed for being operated between 20% and 100% of rated generator power. The controls and operational systems are designed for providing the EPR with a high capacity to follow the actual power demands of the grid. This load follow capability can be shortly summarized as follows:

± 5%/min ramp load change within 50 and 100% thermal power (± 2.5% within 25 and 50%),
± 10% step load change within 20 and 100% power,
+ 20% power increase within 2 minutes,

100-25-100 load follow operation with several load changes per day,

primary and secondary frequency control equivalent to ~ ± 10%.

The load variations can be either initiated by the operator or totally remotely controlled. They do not need any intervention of the operator. The important plant parameters are maintained automatically within operational ranges by control functions. The setpoints for the main NSSS controls (primary coolant temperature, axial power distribution, control rod insertion, primary pressure, secondary pressure, water level in pressurizer and water level in steam generator) are adjusted automatically. The sizing of the plant is done in such a way that during normal plant operation, all the plant parameters are remaining far from the triggering setpoints of any safety system.

Single failures in the I&C will not prevent the plant from operating safely without interruption due to actuation of any safety system.

In addition, the EPR is designed to withstand without tripping the reactor events like:

- Turbine trip,
- Switch-over to house load operation (opening of the grid breakers),
- Loss of a single feedwater pump,
- Malfunction (or switch off) of a single control and parameters approaching safety systems actuation setpoints.

For covering such cases but also erroneous manual actions or strong transients which cannot be easily managed by normal controls, limitation functions are introduced. They are partially independent from the controls and cannot be switched off. They will actuate automatic countermeasures or alarms requiring an operator's intervention with the aim to return the plant parameters within a normal operational range.

A plant surveillance system provides the operator with the information necessary for him to appreciate:

- whether all the systems are operating correctly,
- whether all the plant parameters are ranging within the limiting conditions of operation (LCO). All these measures will contribute to reach the target of less than 1 spurious safety systems actuation/year.

2.2. Automatic safety systems (4.2.2.2)

Principle: Automatic systems are provided that would safely shut down the reactor, maintain it in a cooled state, and limit any release of fission products that might possibly ensue, if operating conditions were to exceed predetermined setpoints.

The EPR design incorporates various safety systems that will act automatically to maintain or to return the plant to a safe condition in case of incidents or accidents initiated either inside or outside the plant. The important safety functions ensured by these systems are:

- Reactivity control,
- Reactor Coolant System (RCS) integrity,
- Reactor Coolant System (RCS) inventory,
- Residual Heat Removal,
- Activity retention and containment integrity.

Reactivity control.

Two independent and diverse means of ensuring control of reactivity, i.e. bringing the reactor to a subcritical state and maintaining its subcriticality, are provided in the EPR, one relying on the rapid insertion of control rods and the other on the injection of boron.

Rapid insertion of control rods is achieved by cut-off of electric power to the rods, thus causing insertion by gravity. The Reactor Protection System provides the necessary instrumentation, signal processing and logic treatment to initiate this action automatically.

Boron injection is provided for by the Chemical and Volume Control System (CVCS) and by the Safety Injection System (SIS). The CVCS provides a sufficient supply of borated water at 7000 ppm to bring the RCS to the cold shutdown boron concentration. The SIS provides capability to inject borated water at about 2000 ppm, taken from the In-Containment Refuelling Water Storage Tank (IRWST), into the RCS at a pressure not higher than the Medium Head SIS pump (MHSI pump) shutoff pressure. Therefore, depressurization of the RCS, together with cooldown via the secondary side will be used to allow initiation of boration by the MHSI. Sufficient shutdown margin is available to allow such cooldown without the need for boration. In addition, letdown of RCS fluid at a small flow rate directly towards the IRWST is used in combination with the MHSI injection to permit achieving cold shutdown boron concentration with the 2000 ppm boron injection flow.

RCS integrity (see also section 2.8).

The automatic systems or actions required to ensure RCS integrity are those intended for overpressure protection and those required for cooling of the Reactor Coolant Pumps (RCP) seals.

RCS overpressure protection is ensured by the three safety valves installed on the pressurizer (see section 2.8).

Cooling of the RCP seals is ensured by injection of a cooled and filtered seal water supply via the CVCS, as well as by the Component Cooling Water System (CCWS). In addition, as a further protection against RCP shaft seal leakage, a standstill seal is provided for the RCP. The standstill seal can be actuated following the shutdown of the RCP and ensures isolation of RCP seal leakage without the need for injection or cooling water supply.

RCS inventory

Normal and emergency makeup to the RCS are provided for by the CVCS and by the SIS.

The CVCS ensures control of RCS inventory during normal operation by maintaining Pressurizer level at the programmed setpoint level through adequate control of charging and letdown flows. Leaks and small diameter piping breaks are also compensated by the CVCS, possibly by startup of a second CVCS charging pump and automatic isolation of letdown flow.

All other incidents or accidents involving larger RCS leakage or larger piping breaks would lead to automatic startup of the SIS. The SIS ensures emergency core cooling for all RCS breaks up to the double ended rupture of a main coolant loop. Low head injection pumps (LHSI), medium head injection pumps (MHSI), and accumulators are available to ensure the required injection flow for the entire range of RCS pressure for all such Loss of Coolant Accidents (LOCAs). The LHSI and the MHSI take suction from the IRWST.

A particular feature of the SIS design for the EPR is the requirement to avoid that, in case of a Steam Generator Tube Rupture (SGTR), excess break flow from the RCS to the affected Steam Generator (SG) would lead to overfilling of the SG and to excess release of contaminated steam or water through the SG relief or safety valves. This is accomplished by setting the shutoff head of the MHSI pumps below the SG safety or relief valve setpoints. At the same time, an automatic cooldown of the secondary side to below the MHSI shutoff head is initiated in case of LOCA, thus ensuring that the required injection by MHSI will be available in all cases, even for small break flow.

For the case of a SGTR, identification of the affected SG by appropriate instrumentation setpoints will then, after automatic isolation of this SG, lead to interruption of any release as well as to termination of break flow towards this SG. Thus excess activity releases and risk of SG overfilling in SGTR transients can be avoided by automatic actions only, without any operator intervention.

During shutdown of the reactor, monitoring and surveillance of RCS inventory will be maintained at all times, and in particular during operation with a lowered level inside the main coolant loops as may occur in a refuelling shutdown outage. The CVCS and the SIS area also available for emergency makeup in such cases.

Residual Heat Removal

Removal of the residual heat produced by fission product decay after a reactor shutdown is ensured at all times, either via the Steam Generators or via heat exchangers located in the Residual Heat Removal (RHR) system, or in the SIS, downstream the LHSI pumps.

Secondary side heat removal via the Steam Generators is used when the RCS temperature is above approximately 150°C. Feedwater supply to the SG is from the normal feedwater system, startup and shutdown feedwater pump, or from the Emergency Feedwater System (EFWS). The steam release from the SG is either via the turbine bypass to the main condenser, or via SG relief valves to the atmosphere. Automatic actuation of feedwater supply and steam release will ensure secondary side heat removal with high reliability, due to the large degree of redundancy and diversity in the feedwater supply and steam release functions.

At lower RCS pressure and temperature conditions the residual heat removal will be via the RHR, so as to enable cooldown to cold shutdown or refuelling shutdown conditions.

In case of a LOCA, the LHSI heat exchangers will be effective to ensure residual heat removal and cooldown of the RCS without exceeding acceptable limits for containment pressure or temperature.

As part of the risk reduction policy (see 1.2-b) heat removal via the SIS is also available in case of a highly unlikely combination of multiple failures leading to complete loss of all secondary side heat removal. In such a case opening of pressurizer safety valves, followed by automatic startup of the SIS will ensure the continued residual heat removal via the primary side.

Activity retention and containment integrity

The confinement of activity is ensured by the containment structure and associated systems ensuring leaktightness, and leak recovery and filtration before stack release. These structures, equipment, and systems are described in sections 2.9 and 2.10. The automatic safety actions which serve to maintain the containment barrier are those that ensure isolation of all containment penetrations, except penetrations serving vital safety functions such as SIS injection, RCP seal water injection and boron injection, and cooling of RCP seals or of RHR heat exchangers. Instrumentation and signal processing are provided to detect conditions requiring such automatic containment isolation.

2.3. Protection against power transient accidents (4.2.3.1)

Principle: The reactor is designed so that reactivity induced accidents are protected against, with a conservative margin of safety.

The EPR is protected against reactivity transients:

a) by inherent negative reactivity feedback,
b) by automatic limitation and safety systems which are introducing neutron absorbers,

c) by specific features minimizing the probability of occurrence of severe reactivity transient.

More specifically, the core design includes the following features:

1) The core is charged mainly with the U^{238} isotope which provides the core with a negative Doppler coefficient. It is designed in addition for having a negative moderator temperature coefficient under normal operating conditions. These both effects provide negative reactivity feedback in case of uncontrolled reactivity excursion.

2) Like other PWRs, the EPR makes use of two means for introducing neutron absorbers in the core: the rod cluster control assemblies (RCCA) and the boric acid diluted in the moderator.

   The RCCA can be inserted in the core only by force of gravity. The drop of all RCCA is actuated by the four fold redundant Reactor Protection System (RPS). The reactor trip function is described in section 2.5. The RCCA system is designed in such a way that, even with the assumptions of the most efficient control rod remaining stuck at its initial position, the shutdown margins are sufficient for demonstrating under conservative assumptions that the design and safety criteria are met for all types of anticipated occurrences and design accident scenarios including overcooling accidents.

   For long term Xe-decay compensation and plant cooldown the increase of the boric acid concentration is needed. The boration function is normally ensured by the Chemical and Volumetric Control System (CVCS). In case of the loss of the CVCS, the boration function can be ensured by the Safety Injection System (SIS) which is a safety grade system injecting borated water of the IRWST after a primary bleed was actuated manually.

3) The probability of occurrence of severe reactivity transients and the potential reactivity addition rates are minimized by the following EPR features:

- Under critical conditions at zero power or part load, the control rods are always inserted only to the extent necessary for increasing the power up to 100%. At 100% the control rods are nearly withdrawn. Uncontrolled rod withdrawal will not jeopardize the fuel integrity.

- The reactivity addition rate due to RCCA withdrawal is limited by means of RCCA power supply configuration and capacity. The rods cannot be moved simultaneously. In addition, the withdrawal speed is limited by the I&C.
- Unallowed escalation rates of neutron flux signals or power levels or overshooting of neutron flux or power levels thresholds are detected and limitation functions are actuated automatically. Blocking RCCA extraction and isolating demineralized water injection are typical countermeasures to stop the neutron flux increase. In case the limitations are not efficient enough, a reactor trip is actuated.

2.4. Reactor core integrity (4.2.3.2)

Principle: *The core is designed to have mechanical stability. It is designed to tolerate an appropriate range of anticipated variations in operational parameters. The core design is such that the expected core distortion or movement during an accident within the design basis would not impair the effectiveness of the reactivity control or the safety shutdown systems or prevent cooling of the fuel.*

The fuel assemblies of the EPR will be of proven design. This design will be the result of the evolution of the technology for nuclear fuel experienced on existing PWR plants.

This fuel is of the type 17 x 17 and will be designed to reach a batch burnup of 60 MWd/kg HM.

The reactor (core and systems) is designed in such a way that depending on the plant condition categories the following safety criteria are met:

Plant condition categories	Core specific safety criteria
PCC 1 normal operation	No additional* fuel damage
PCC 2 anticipated operational occurrences	No additional* fuel damage triggered by this type of events * *additional is mentioned as a small amount of defects that could be tolerated, compatible with the capacity of the cleanup system*
PCC 3 Infrequent accidents	Return to safe state after the accident: only a very small number of fuel rods is damaged. (except for secondary side breaks or steam generator tube rupture for which no rod damage is accepted)
PCC 4 Limiting accidents	Return to safe state after the accident ; The core can be cooled and can be kept subcritical. The number of damaged rods is < 10% (except for secondary breaks for which no rod damage is accepted)

2.5. Automatic shutdown systems (4.2.3.3)

Principle: *Rapidly responding and highly reliable reactivity reduction for safety purposes is designed to be independent from the equipment and processes used to control the reactor power. Safety shutdown action is available at all times when steps to achieve a self-sustaining chain reaction are being intentionally taken or whenever a chain reaction might be initiated accidentally.*

The essential automatic shutdown system used to interrupt the chain reaction is the so-called reactor shutdown system (reactor trip function). The operation of the system consists of dropping all the Rod Cluster Control Assemblies (RCCA) in the core. This dropping occurs only by gravity after the rod drive mechanism have been de-energized. The actuation of the reactor trip function is totally independent, from the mechanical and I&C point of view, from the manual or automatic RCCA step by step movements. It remains active until it is disabled by manual intervention by the operator after the cause of its actuation is identified and corrected. The safety I&C which is opening the breakers for de-energizing the rod drive mechanism is based on a four fold redundant I&C structure using a "2 out of 4" logic for coping with a single failure during maintenance. The four redundant divisions are independent, physically separated and electrically isolated.

For most of the events requiring the actuation of the reactor trip, physically diverse initiation channels are used. Where this functional diversity cannot be found, if necessary to meet the probabilistic targets, diversity will be introduced by selecting diverse sensors for the same parameters.

Obviously, safety I&C and operational I&C are normally separated. It is ensured by specific means that orders from the safety I&C have priority against orders from the operational I&C. This prevents failures in the non safety I&C to disturb the operation of the safety grade I&C.

Due to the I&C organization used for safety grade systems, the reactor trip function has a very high probability of performing the reactor shutdown on demand.

Some very unlikely events, considering that the shutdown would not be effective due to common cause failure postulates like mechanical blocking of the RCCAs, are nevertheless studied (ATWT). In this case, boration functions are used for reaching subcritical conditions.

Boration functions are used also for reaching cold and/or long term safe subcritical conditions.

2.6. Normal heat removal (4.2.3.4)

Principle: *Heat transport systems are designed for highly reliable heat removal in normal operation. They would also provide means for the removal of heat from the reactor core during anticipated operational occurrences and during most types of accidents that might occur.*

The heat transport paths foreseen for the EPR make use of the Steam Generators, during normal power operation, and hot and intermediate shutdown states, and of the RHR system, during the cold shutdown state and refuelling periods.

Reliable operation of the secondary side heat removal is achieved by reliance on redundancy and diversity in the design of the feedwater supply and of the SG steam release functions.

The normal feedwater supply is from either the Main Feedwater Supply system, or the Startup and Shutdown System (SSS), thus ensuring highly reliable SG feeding and minimizing the frequency of events where emergency feed via EFWS would be required.

The steam produced in the SG will during normal power operation be directed towards the turbine, while during shutdown the turbine bypass to the main condenser will permit reliable continued steam and heat removal.

Normal cold or refuelling shutdown heat removal is via the RHR system. The RHR is composed of two separate trains, located inside the containment. This location eliminates any risk of containment bypass in case of leaks or ruptures in the RHR system during its operation. Below 100°C and at reduced RCS pressure two of the four LHSI trains and their heat exchangers may also be used for RHR duty, thus ensuring a large degree of redundancy and diversity.

2.7. Emergency heat removal (4.2.3.5)

Principle: *Provision is made for alternate means to restore and maintain fuel cooling under accident conditions, even if normal heat removal fails or the integrity of the primary cooling system boundary is lost.*

In case plant incidents or accidents would render unavailable the normal means of heat removal listed in section 2.6 above, alternate emergency heat removal systems will ensure that core cooling is maintained. Such emergency heat removal means have already been identified in section 2.2, in the description of automatic safety systems: SG heat removal is ensured by the EFWS and SG relief and safety valves, while primary side heat removal is ensured by RHR, and SIS.

The EFWS is composed of four completely separate and independent trains, each feeding into one SG. Each train comprises an emergency feedwater tank, an emergency feedwater pump, and associated piping and valves feeding into a separate, dedicated inlet nozzle of the SG. The EFWS pumps are motor driven and are supplied each by its associated train of emergency electric power supply. Diverse emergency electric generators will be used. The redundancy and diversity in the various normal and emergency sources of feedwater supply will thereby guarantee the required high level of reliability of secondary side heat removal (see also section 2.13).

In accidents involving a loss of integrity of the primary coolant system boundary, (i.e. LOCA) emergency heat removal will be ensured by the SIS for the intermediate and large break LOCA, and by both SIS and secondary side SG cooling for the small break LOCA. This is made possible by the heat exchangers arranged in the LHSI injection path of the SIS.

The SIS is composed of four completely separate and independent trains, each ensuring injection by medium and low head pumps, (MHSI and LHSI), as well as an accumulator which will inject automatically in case of a decrease in RCS pressure following a LOCA. As for the EFWS, each SIS train is supplied with electric power from its associated train of the emergency electric power supply system. The LHSI and MHSI take suction from the IRWST and inject into RCS hot and cold legs (MHSI in cold legs, LHSI in both hot and cold legs). The accumulator injection is in the hot leg. Adequate sizing of injection ensures rapid core quenching and reflooding even for the largest possible RCS loop break size.

As mentioned in section 2.2, the primary side heat removal via SIS can also be made available in the highly unlikely event of a complete failure of all secondary side heat removal.

This "feed and bleed" mode of operation requires opening of the pressurizer safety valves which, after decrease of RCS pressure as a result of safety valve discharge, will lead to automatic actuation of SIS so that continued core cooling and decay heat removal is ensured.

During shutdown conditions the heat removal path is normally via RHR. In case of failures that would lead to a complete loss of RHR, emergency heat removal is possible either by returning to the secondary side heat removal mode via SG, or by making use of connections to two of the four LHSI pumps and heat exchangers, which are specifically provided for this purpose. The return to SG heat removal is used when RCS temperature is above 100°C, while use of LHSI as alternate heat removal means can be employed at RCS temperature below 100°C. A gross leakage or large rupture of the RHR during its operation would lead to emergency injection and heat removal by the SIS, in the same manner as for the LOCA accidents.

2.8. Reactor coolant system integrity (4.2.3.6)

Principle: *Codes and standards for nuclear vessels and piping are supplemented by additional measures to prevent conditions arising that could lead to a rupture of the primary coolant system at any time during the operational life of the plant.*

The reactor coolant pressure boundary is designed, manufactured and tested in compliance with the class 1 requirements of the ETC-M code[1].

Structural design

Conservative operating transients (severity, number of occurrences) and loads are considered to demonstrate structural integrity over a 60 years life. Mechanical damage such as fatigue, excessive or progressive deformation, are prevented by strict compliance to conservative rules and stress criteria. Corrosion and stress corrosion cracking phenomena are prevented by proper selection of materials. Special rules apply to the Reactor Pressure Vessel (RPV) core shell region as addressed below.

Crack growth analysis are performed for typical parts to prove low propagation of defects assumed to survive the non destructive tests conducted in shops and on site. Fracture mechanics analysis demonstrates large margins against catastrophic failure even under extreme loads. A break preclusion concept, which includes Leak Before Break (LBB), is implemented on the main coolant lines.

Extreme loading conditions are postulated to design the components, their supports and anchors into the civil structures such as earthquake and pipe breaks. In particular earthquake loads are defined for a wide range of soil conditions and earthquake parameters.

[1] ETC's (European Technical Codes) are a set of common rules elaborated within the frame of the Franco German cooperation. They are substantially based on the German KTA and French RCC rules. The ETC-M covers the mechanical component pressure boundary.

Materials and product forms

The material used for the pressure boundary are the same grades as used on French and German operating plants i.e. either a low alloy ferritic steel or a low carbon austenitic steel (stabilized or not). These materials have excellent toughness properties and are easily weldable.

With the possible exception of the Reactor Coolant Pump (RCP) casing and valves bodies which may be cast, all parts are forged. In particular the Main Coolant Lines (MCL) are entirely made of forged parts. The number of welds is minimized to enhance mechanical reliability and reduce In Service Inspection (ISI).

Claddings are made of low carbon austenitic steel (stabilized or not). Intergranular corrosion is therefore excluded. Inconel welds between austenitic steel and carbon steel are made with a Stress Corrosion Cracking (SCC) free material (Inconel 182 or 152).

Proper welding conditions (preheating and postheating) exclude hydrogen induced failure mechanism.

The Steam Generator (SG) tube material can be either Inconel 690 or Incolloy 800. Both material have adequate corrosion resistance and are offered as options.

In-service inspection

All parts being forged (except possibly RCP casing) ISI can be performed by Ultrasonic Testing (UT) including the MCL. Grain size in austenitic forged parts is specified for that purpose. Radiographic examination of the large welds between the MCL and the heavy components may also be performed if preferred layout provisions are implemented for easy access to the component outside surface and for installation of rails for automatic UT inspection of the MCL, the SG (including secondary side), and the pressurizer.

Replaceability

All components and supports are replaceable, except the RPV main body and its supports.

Leak detection

The RPV and RCP flanges are equipped with two gaskets with a leakage alarm between the two. An ambient leak detection system with sensors located in several compartments, monitors physical parameters which are relevant to a primary coolant leak (temperature, activity). Other means are also available to detect and measure a large leak (water level, balance of flow).

Activity of the secondary side of the SG is monitored for detection of any leak from the primary side.

Overpressure protection

At least three discharge trains are installed at the pressurizer. Each discharge train is provided with two safety valves in series thus ensuring possibility of isolation of a stuck open valve. The units are designed and qualified for both steam, water, and for two phase flow discharge conditions, as well as for discharge of fluid containing increased quantities of non-condensable gases.

Reactor pressure vessel integrity

The fracture toughness properties of the base material, the weld and the Heat Affected Zone (HAZ) are specified in compliance with the ETC-M for all components. In addition to the fabrication and testing measures which minimize the probability for a defect on any component, special requirements apply to the beltline region of the vessel.

The RPV integrity is additionally ensured by three combined means:

- high initial toughness properties. This is achieved through additional requirements on impurities and material homogeneity.
- a low RTndt shift over the 60 years design plant life. The fluence is limited by design to 10^{19}nvt, and stringent requirements on impurities influencing the toughness shift under irradiation are implemented.
- safety injection water is stored inside the containment and shall be above 25°C.

A material surveillance program to monitor the effects of irradiation on material properties is included in the EPR.

2.9. Confinement of radioactive material (4.2.3.7).

Principle: *The plant is designed to be capable of retaining the bulk of the radioactive material that might be released from fuel, for the entire range of accidents considered in the design.*

The EPR plant design incorporates a double containment concept which will be capable of retaining radioactivity releases from the fuel and the RCS system boundary during any incident or accident considered in the Plant Condition Categories (PCC) of the deteministic design basis (see 1.2-a), as well as the releases that would occur during the more severe conditions considered as part of the risk reduction strategy (see 1.2-b), and which include accident sequences and scenarios involving a core melt.

The double wall containment consists of:

- an inner wall of prestressed concrete without liner,
- an outer wall of reinforced concrete,
- a basemat of reinforced concrete.

In this concept the structures and systems contributing to the containment function comprise:

- the inner and outer containment and the space between them, which is designated as the annulus. This annulus is maintained at a subatmospheric

pressure in order to collect all possible leaks through the inner wall and filter them before release to the stack,
- systems required for isolation and for retention and control of leakages,
- systems required to maintain pressure and temperature conditions inside the containment within limits compatible with leaktightness and structural integrity of the containment.

All system penetrations through the containment inner wall are provided with isolation valves, either locked closed or automatically closing in case of an accident. Double isolation valves are foreseen, unless the system provides a closed pressure boundary inside or outside the containment.

The containment leak collection strategy is as follows:

- Leakages are in principle collected within the annulus either directly or via leakage control measures.
- Components and systems which penetrate the confinement boundary will be designed leaktight.
- Leakage collection is in addition foreseen for openings for equipment and personnel access, equipped with hatches or locks, as well as for ventilation system penetrations, which are open to the containment atmosphere. All such penetrations or openings, which are maintained closed during normal reactor operation, will be provided with sealing devices allowing collection of leakages ensuring filtered release to the plant stack.
- If, nevertheless, leakages have to be considered, they will be collected in the surrounding buildings (ventilation, deposition).

Pressure and temperature conditions inside the containment are maintained within design limits by heat removal systems which, for the case of Plant Condition Categories (PCC) included in the deterministic design basis, comprise the ventilation systems foreseen for normal operation, the thermal inertia of the containment structures, and the heat exchangers arranged in the LHSI flowpath. The LHSI is in particular the principal mode of containment heat removal in case of LOCA. For the more severe accident scenarios, including core melt conditions, a separate, completely independent Containment Heat Removal System (CHRS) is provided. The CHRS is composed of a spray system, arranged in two trains, and will ensure a heat removal capacity sufficient to prevent a containment pressure increase above 7.5 bar, when the system is started after a time delay of approximately one half to one day following accident initiation. This grace period permits CHRS actuation to be by manual operator intervention only, from the main control room.

The containment design pressure is set at 7.5 bar, providing a comfortable margin above the maximum pressure expected for the PCC design basis accidents (LOCA or Steam Line Break), which is in the rang the of 5.5 bar, and ensuring the necessary resistance and grace period for compatibility with CHRS design in the more severe accident scenarios. Leaktightness of the containment will be guaranteed at this pressure level, and will be monitored by integral leak rate test in an air atmosphere at the same pressure level of 7.5 bar absolute.

2.10. Protection of confinement structure (4.2.3.8)

Principle: If specific and inherent features of a nuclear power plant would not prevent detrimental effects on the confinement structure in a severe accident, special protection against the effects of such accidents is provided, to the extent needed to meet the general safety objective.

One of the most important objectives of the EPR is the limitation of large releases to a frequency lower than 10^{-6} per reactor - year.

The consequence on the plant design is the consideration of severe accident conditions, including core melt.

More specifically, this means that a prevention strategy is used to ensure that accident sequences leading to early containment failure, such as core melt at high RCS pressure, or associated with containment bypass are made sufficiently unlikely (i.e. below the large release frequency limit), while a mitigation strategy is used to ensure compliance with release limits in the case of a low pressure core melt sequence. The main features contributing to this mitigation are shortly described below.

- A cylindrical double containment concept has been adopted for the EPR which includes an inner prestressed concrete vessel. Its design pressure is set at 7.5 bar (absolute), so as to allow adequate margin enveloping the severe accident scenarios envisaged. Recombiners and possibly igniters will be used to ensure that pressure due to hydrogen burning or deflagration will be below this design value.
- A dedicated containment heat removal system (spray in the containment atmosphere and long term subcooling of the sump water by recirculation) is provided for long term containment cooling. Due to the increased containment design pressure, a grace period between about 0.5 and 1 day will be available before manual initiation of this function is required. No filtered vent system is therefore necessary.
- A basemat protection is provided, since a Reactor Pressure Vessel failure has to be considered. Therefore, below the vessel and on the side of the reactor cavity, the core melt will be spread over a large area and quenched by water available in the refuelling water storage tank arranged inside containment (IRWST). This will ensure long term cooling of the spreaded core melt in a stable configuration.

2.11. Monitoring of plant safety status (4.2.3.9)

Principle: Parameters to be monitored in the control room are selected and their displays are arranged to ensure that the operators have clear and unambiguous indications of the status of plant conditions important for safety, especially for the purpose of identifying and diagnosing the automatic actuation and operation of a safety system or the degradation of the defence in depth.

Overall description of the Main Control Room

The Main Control Room (MCR) of the EPR is a screen based control room with an overview panel and is used for process control during normal operation including outages and accidental situations.

The MCR contains at least 3 operator work positions (all of the same design) which are used for process control in all plant conditions via operational I&C. In addition, the MCR has a safety control area with back up control means.

These operator work positions are dedicated to:

- the primary loop operator,
- the secondary loop operator,
- the auxiliary operation or back up purposes.

A shift supervisor console offers operational and safety-qualified information to the shift supervisor and to the safety engineer. It is equipped with communication means and space for administrative work.

A plant overview panel, consisting of a permanent display of the main circuits and plant parameters and of a variable part allowing the display of any graphic of the process information system is visible from all workplaces and will be used for the coordination among the operators and for the transfer between normal and back up means.

The safety control area (back up control means) in the MCR is used in the case of major losses of the normal control means. It can be used for the safe shutdown (hot or cold) of the plant or to perform post-accident operation.

The safety control area constitutes a safety relevant man machine interface. The related equipment is qualified accordingly.

Alarms

The alarm processing and presentation is conceived in order to minimize non-significant or redundant alarms. The purpose is to alert the operator only if it is necessary for him to perform any corrective action, or to be aware of a change of the state of the plant.

A classification of alarms is introduced, based on the urgency of the operator action, the relevance to safety, and the consequence on function availability.

Their presentation will allow the operator to determine immediately if a corrective action has to be performed, what is the degree of urgency and whether there is an impact on the safety of the plant.

Alarms will be presented to the operator in three ways:

1) Presentation on alarm screens in form of sorted lists, in order to avoid an alarm avalanche to the operator; this presentation is affected by the suppression of alarms according to the plant state and the suppression of alarms which

are consequence of an event already indicated by another alarm. In addition, the list of suppressed alarms is available on demand.

2) Presentation on screen in text or symbolic form with detailed information graphics representing systems and functions, thus allowing to interpret the alarm within the context of the system or function it originates from.

3) Presentation on screen in overview synthesis graphics: alarms influence the appearance of graphics or text symbols in overview information graphics representing:

   - the status of all the plant functional groups, including the degree of disturbance (in operation, locally disturbed, function in danger, partial failure, failed)
   - the status of safety objectives (subset or all criteria fulfilled),
   - the automatic detection of accident situations,
   - an indication of the presence of alarms not contained in the list above and present in the alarm list.

Changes of signals for alarms or of the status of function/systems are announced by optical/acoustic means. As far as acknowledgement of alarms is required, it can be performed through the alarm screen as well as through the function/systems oriented information graphics.

2.12. Preservation of control capability (4.2.3.10)

Principle: *The control room is designed to remain habitable under normal operating conditions, anticipated abnormal occurrences and accidents considered in the design. Independent monitoring and the essential capability for control needed to maintain ultimate cooling, shutdown and confinement are provided remote from the main control for circumstances in which the main control room may be inhabitable or damaged.*

The main control room of the EPR is placed in a bunkered building to be protected against external hazards.

The unavailability of the main control room (e.g. by fire) is nevertheless considered but not concurrently with an accident situation. A remote shutdown station (RSS) is implemented which contains the necessary controls and information means to transfer and maintain the plant in safe shutdown conditions. These means are essentially identical to those used in the MCR. The RSS has priority over the control means of the MCR. The RSS control means are isolated for avoiding spurious orders from the MCR.

2.13. Station blackout (4.2.3.11)

Principle: *Nuclear plants are so designed that the simultaneous loss of normal on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage.*

The onsite electric power supply for normal and emergency consumers for the Nuclear Island is arranged in a four train configuration, each train being installed in a separate layout division. Power supplies for users in the Conventional Island are installed in a separate conventional electrical building. Two connections to the offsite network are foreseen, one via the generator, and one via a second offsite grid connection. Emergency busbars are in addition supplied with power from four Emergency Diesel Generators, one for each train. Batteries are foreseen to ensure supply for low voltage consumers which require uninterrupted power supply, in particular I&C. All systems and components required for bringing the plant to cold shutdown, maintaining cold shutdown, and for system operation following incidents or accidents are supplied from the emergency busbars. Therefore, in the event of a loss of offsite and onsite power supply, the diesel generators provide capability to ensure plant safety.

Attention will be paid specifically to the design of the emergency diesels to ensure highly reliable emergency power: diverse equipment design and manufacturing will be employed, so that two of the four diesel generators will be of a design diverse relative to the two others. This will permit a level of reliability which is adequate to ensure that a total loss of both onsite and offsite power supplies as well as of all four emergency diesels will be sufficiently unlikely to avoid the need for other power sources.

2.14. Control of accidents within the design basis (4.2.3.12)

Principle: *Provisions are made at the design stage for the control of accidents within the design basis, including the specification of information and instrumentation needed by the plant staff for following and intervening in the course of accidents.*

General EPR approach

As described in 1.2, the safety approach for the EPR includes a strong deterministic basis complemented by probabilistic analyses in order to improve the prevention of accidents as well as their mitigation.

Only the deterministic approach is addressed in this chapter. The deterministic approach which is founded on the defence in depth principle implies the identification and classification of events liable to occur at the plant due to Internal Events or Hazards or to External Hazards. As a general application for the design of the components, structures and systems: the higher the probability of occurrence of an event, the lower the consequences in terms of unavailability, damages, and radioactive releases.

Safety principles applicable to the design of structures, systems and components:

In conformity with the first level of the defence in depth, the safety requirements are considering first the prevention of the accidents, particularly any which could be initiators of severe core damage or large releases. The first means to achieve this prevention is to strive for such high quality in design, construction and operation of the plant that deviations from normal operational states are infrequent. The defence in depth also includes the mitigation of accidents, in order to further decrease the likelihood of a Severe Accident or of large releases. In such circumstances, safety features would act to confine any radioactive material released from the core so that discharge to the environment would be limited.

These safety features include physical barriers, some of which have the single purpose of confining radioactive material. The requirements imposed on these barriers shall consider the reactor core and the spent fuel storage. Liquid and gaseous effluent storage are treated according to their activity inventory and their storage conditions. Safety systems and the associated I&C make use of redundancy and diversity, and the physical or geographical separation of parallel components to reduce the likelihood of the loss of a vital safety function. Systems and components will have to be inspected and tested regularly to reveal any degradation which might lead to abnormal operating conditions or inadequate safety system performance.

Systems and components will be designed, constructed and tested according to quality standards commensurate with their safety importance. The corresponding rules will preferably be based on experience from earlier operating plants.

The criteria applicable for the design are considering the following principles mainly directed to the systems:

- simplicity and functional separation,
- redundancy and diversity where this is justified from the probabilistic point of view,
- divisional separation of redundant trains including power supply, I&C, and supporting features like cooling water and ventilation,
- low sensitivity to failures (adequate margins, automation, grace period).

Definition of Plant Condition Categories (Deterministic design basis)

The choice of the events to be considered for the NI design and safety assessment is firstly done deterministically. They consist mainly of the normal operational states which are foreseen for normal plant operation and are enlarged by systematically looking for events having the potential of disturbing:

- the reactivity power control,
- the heat removal from the fuel elements,
- the confinement of radioactivity.

A number of representative postulated initiating events (PIE) is derived from this systematic approach which identify bounding cases for design and assessment of safety-classified systems, components and structures. According to their roughly expected frequencies, the events are categorized in 4 categories:

- Plant Condition Category (PCC) 1 : Normal Operation
- Plant Condition Category (PCC) 2 : Anticipated Operational Occurrences
- Plant Condition Category (PCC) 3 : Infrequent Accidents
- Plant Condition Category (PCC) 4 : Limiting Accidents

In order to keep the risk correlated with PCC1 to 4 acceptable, it is required that more likely events lead to lower radiological consequences.

Design basis and control of accidents

Normal operation states (PCC1) are corresponding to states expected regularly or frequently in the course of the normal plant operation.

For most of the normal operation states, the operating parameters are kept within their control range by automatic controls. Additionally, limitation functions ensure that the plant parameters are maintained within certain limits called "Limiting Conditions of Operation" (LCOs). Information systems provide the operator with all the information necessary to be informed about the convenient operation of all systems.

The most penalizing states within LCOs are taken as initial conditions for the accident analyses and for designing the safety systems. Concerning the hypotheses and the characterization of the systems involved in the accident analyses, conservative data are assumed. In addition to the PIE, single failure modes are postulated for the systems used to mitigate the accident.

For the EPR, two phases are considered in the accident evolution:

- The automatic phase which spans from the PIE occurrence up to the first manual action.
- The earliest manual action is supposed to take place 30 minutes after the first significant information are given to the operator.
- The manual phase which spans from the first manual action up to the safe shutdown conditions.

The automatic phase as well as the operator actions, which consist in applying the suitable emergency operating procedure (EOP), are relying on appropriately designed systems: fluid systems, I&C, power supply and supporting systems.

As far as the man-machine interface is concerned, due consideration will given to the human factor at the design stage, taking into account aspects of operation, testing and maintenance. The general aim is to minimize the possibilities for operator errors. This is achieved by applying appropriate ergonomic design principles and by providing sufficiently long grace periods for the operator responses. The necessary length depends on the complexity of the situation to be diagnosed and on the actions to be taken (pre-planned, in the control room, at different locations).

The following grace periods for interventions are used within the deterministic Design Basis:

- main control room actions	> 30 min.
- local actions	> 1h

and for potential Risk Reduction measures :

- use of portable equipment	> 6h
- use of heavy additional equipment	> 3 days

Sufficient and appropriate information will be made available to the operator for a clear understanding of the plant status, including Severe Accident conditions, and for the clear assessment of the effects of his interventions. Emphasis will be placed on the use of computer techniques for reliable diagnosis systems for operator support.

The man-machine interface (MMI) concept for process and accident control respects the properties and abilities of the operator, and brings the capabilities of I&C for operational and safety tasks in an optimum way into action without overloading the operator.

The MMI facilities are subdivided into the following main items:

- the central permanently manned Main Control Room designed for
  - power operation including power changes and stretch-out operation,
  - startup and shutdown phases,
  - disturbances and accidents,
  - outages, e.g. refuelling,
  - service, maintenance and tests.
- the Remote Shutdown Station manned on demand in case of unavailability of the Main Control Room, and
- local control stations manned on demand.

2.15. Mitigation and control of severe accidents

General EPR approach

The safety approach of the EPR is based, as described in 2.2 on a two-fold strategy which consists first in designing the plant with a strong "Deterministic Design Basis" for reducing the probability of accident scenarios and second in implementing right from the beginning additional features to mitigate the consequences of severe accident scenarios, even if their probability of occurrence can be considered very low.

Safety principles applicable to the design of structures, systems and components

For the design of the EPR, beyond the Plant Condition Categories (PCC) 1 to 4 which are in a classical way used for defining and sizing the safety systems, two additional "Risk Reduction Categories" RRC-A and RRC-B were introduced for preventing respectively core melting and large activity releases. Within these two last categories, events with multiple failures and coincident occurrences up to the total loss of safety systems are considered on a probabilistic basis, and the systems are designed in such a way that integral probabilities for core melting or large releases will remain respectively below 10^{-5}/reactor x year and 10^{-6}/reactor x year.

This method will allow to implement, to design and to arrange all the systems and equipment necessary for the mitigation and the control of RRCA and B events in a comprehensive and balanced way, avoiding overdesign in some places or weak points in some others.

Typical features which are introduced are the following:

- primary discharge into the containment water storage tanks in the case of total loss of secondary side cooling,
- introduction of systems diversity and/or back up functions for coping with common cause failures on components, systems or I&C,
- features for spreading and cooling the corium, for recombining hydrogen and for containment heat removal in case of core melt,
- appropriate information display and operator aid for allowing the long term accident management (This part is already developed in the previous section 14).

3. LIST OF MAIN PARAMETERS (PRELIMINARY)

Station output		
Nuclear Power	MWth	4250
Gross electrical rated power	MWe	1500
Reactor core		
Number of Fuel Assemblies		241
Type of Fuel Assemblies		17 x 17
Active length	mm	4,200
Total Fuel Assembly length	mm	4,800
Linear Heat Rate	W/m	15.5
Number of Control Rods		81
Total Flow Rate (T.H. - Design Cond.)	kg/s hot	21 050
(B.E. - Design value)		21 900
Vessel Inlet/Outlet Temp. (T.H. Cond.)	°C	291/326
Enrichment (max) % U^{235}		4.9
Batch discharge burnup	MWd/kg	60
Mox - capability		yes
Primary and Secondary system basic data		
- RCS operating pressure	MPa	15.5
- RCS design pressure	MPa	17.6
- SG tube bundle outlet pressure at 100%	MPa	7.25
- Main steam pressure at hot standby	MPa	8.4
- Secondary side design pressure	MPa	9.1-9.4

Cont.

Primary Components	
Reactor Pressure Vessel	
- Fluence (design target - 60 years)	1.10^{19} nvt
- Material	16MND5/20MnMoNi55
- Nozzles	set on
- Support	underneath the nozzles
Steam Generator	
- Heat transfer surface m^2	7300 (with economizer)
- Tube material	Incolloy 800 or Inconel 690
- Pressure boundary material	16MND5/20MnMoNi55
- Water amount secondary side at full load t	~ 75
Pressurizer	
- Pressure boundary material	16MND5/20MnMoNi55
- Total volume m^3	~ 75
Reactor Coolant Pump	
- Suppliers	Framatome or KSB
- Casing steel	Stainless or Ferritic with cladding
- Shaft seals	3 seals, Standstill seal
Main Coolant Line	
- Material	Forged ferritic with cladding or Stainless steel

Cont.

Containment	
Free volume m^3	75 000
- Design pressure for DBAs bar abs	- LOCA or steam line break app. 5.5 (0.55 MPa)
- Design pressure for severe accident bar abs	app. 7.5 (0.75 MPa)
- Test pressure bar abs	app. 7.5 (0.75 MPa)
- Integral leakrate for primary wall	< 1% vol/day
Civil Works **Protection against External Hazards**	
Safe Shutdown Earthquake (SSE)	USNRC spectrum/0.25g
Airplane Crash (APC)	80 MN
Explosion Wave (EPW)	100 mbar (10 kPa) incoming wave
Reactor Building	
SSE	yes
APC	yes
EPW	yes
Safeguard Building	
SSE	yes
APC	partial
EPW	yes
Fuel Building	
SSE	yes
APC	yes
EPW	yes

BASIC INFORMATION ON DESIGN FEATURES OF THE AP600

B. A. MCINTYRE
Energy Systems, Westinghouse Electric Corporation,
Pittsburgh,
USA

Presented by E. Mink

Abstract

The paper describes the AP 600 (Advanced Passive Pressurized Water Reactor) power plant design of Westinghouse Electric, USA. The paper consists of three parts: - a general description of the plant concept; - a description of how the plant compares with the safety principles of INSAG-3 for 15 selected design areas;, and - an extended data list. The general description outlines the plant design basis, describes main features of the reactor plant and its safety systems, simplifications and introduction of passive safety and digitized instrumentation & control systems, and discusses defense-in-depth aspects. The second part discusses plant performance in the areas of: - plant process control systems; - automatic safety systems; - protection against power transient accidents; - reactor core integrity; - automatic shutdown systems; - normal heat removal; - emergency heat removal; - reactor coolant system integrity; - confinement of radioactive material; - protection of confinement structure; - monitoring of plant safety status; - preservation of control capability; - station blackout; - control of accidents within the design basis; and - mitigation and control of severe accidents. The third part, finally, presents data related to the power plant as a whole, data on reactor core and reactivity control, on the reactor coolant system, the reactor pressure vessel, steam generators, pressurizer, and main coolant pumps, on the containment, and on safety systems or safety-related systems.

1. GENERAL DESCRIPTION OF AP600

1.1. Plant design basis

Through the very broad participation of numerous countries, the wealth of information that has been generated worldwide relating to nuclear power plant safety and operations has been focused in the EPRI's ALWR Utilities Requirements Document (ALWR URD). The purpose of the URD is to present a clear, complete statement of utility desires for their next generation of nuclear plants, and to this end, it consists of a comprehensive set of design requirements for future plants. These requirements are grounded in the proven technology of over 30 years of commercial U.S. and international experience, while incorporating new features that ensure a simple, robust, and more forgiving design.

Incorporation of the ALWR URD has been a key design goal for the AP600 from design inception, during implementation, and beyond the First-of-a-Kind Engineering (FOAKE) Program.

The AP600 has a well-defined design basis that is confirmed through thorough engineering analyses and testing and is in conformance with the Utility Requirement Document (URD). Some of the high-level design bases that characterize the plant are:

- Net electrical power at least 600 MWe with a nuclear steam supply system power rating of 1940 MWt.

- Designed for rated performance with up to 10% of the steam generator tubes plugged and with a maximum hot leg temperature of 600°F (315.6°C).
- Robust core design with at least a 15% operating margin on core power parameters.
- Five-year lead time (owner's commitment to commercial operation) and a 3-year construction schedule.
- No plant prototype required based on use of proven power generating system components.
- Passive safety systems that require no operator action for 72 hours post accident, and maintain core and containment cooling indefinitely without ac power.
- Predicted core damage frequency <10E-05/yr, and significant release frequency <10E-06/yr.
- Standard design applicable to anticipated U.S. sites.
- Occupational radiation exposure < 70 man-rem/yr (0.7 man-Sv/yr).

- Designed for an 18-month fuel cycle assuming an 85% capacity factor; capable of a 24-month cycle.
- Refueling outage free from major problems can be conducted in 17 days or less (breaker to breaker).
- Plant design objective of 60 years without the planned replacement of the reactor vessel.
- Overall plant availability goal greater than 90% considering forced and planned outages. Goal for unplanned reactor trips less than one per year.

1.2. Simplified reactor coolant system (RCS)

The AP600 RCS includes features based on existing technology that significantly and measurably enhance plant reliability, simplicity of operation, and plant safety, as compared with conventional pressurized water reactor (PWR) plants. The RCS is configured to take advantage of lessons learned from previous power plants. Furthermore, the design incorporates the ALWR utility requirements and satisfies all general design criteria of 10 CFR 50, Appendix A.

Reactor Design.

The core, reactor vessel, and reactor internals of the AP600, shown in Figure 1, are similar to those of a conventional Westinghouse PWR design. Several important features based on existing technology measurably enhance performance characteristics as compared with conventional plants. The reactor core is a low-power density design that uses the Westinghouse 12 foot (3,658 mm), 17×17 fuel assembly. The fuel assembly is based on the proven Westinghouse VANTAGE 5H design, which is used in 20 percent of all current Westinghouse reactors. Low-power density is achieved by making the core larger than previous 600 MWe designs, with the number of fuel assemblies increased from 121 to 145. This configuration results in core power density and average linear power density enhancements of about 25 percent over conventional plants of the same power rating. This results in lower fuel enrichments, less reliance on burnable absorbers, and longer achievable fuel cycles.

RCS Piping and Loop Layout.

The RCS loop layout contains several important features that provide for a significantly simplified and safer design. The reactor coolant pumps (RCPs) mount directly on the

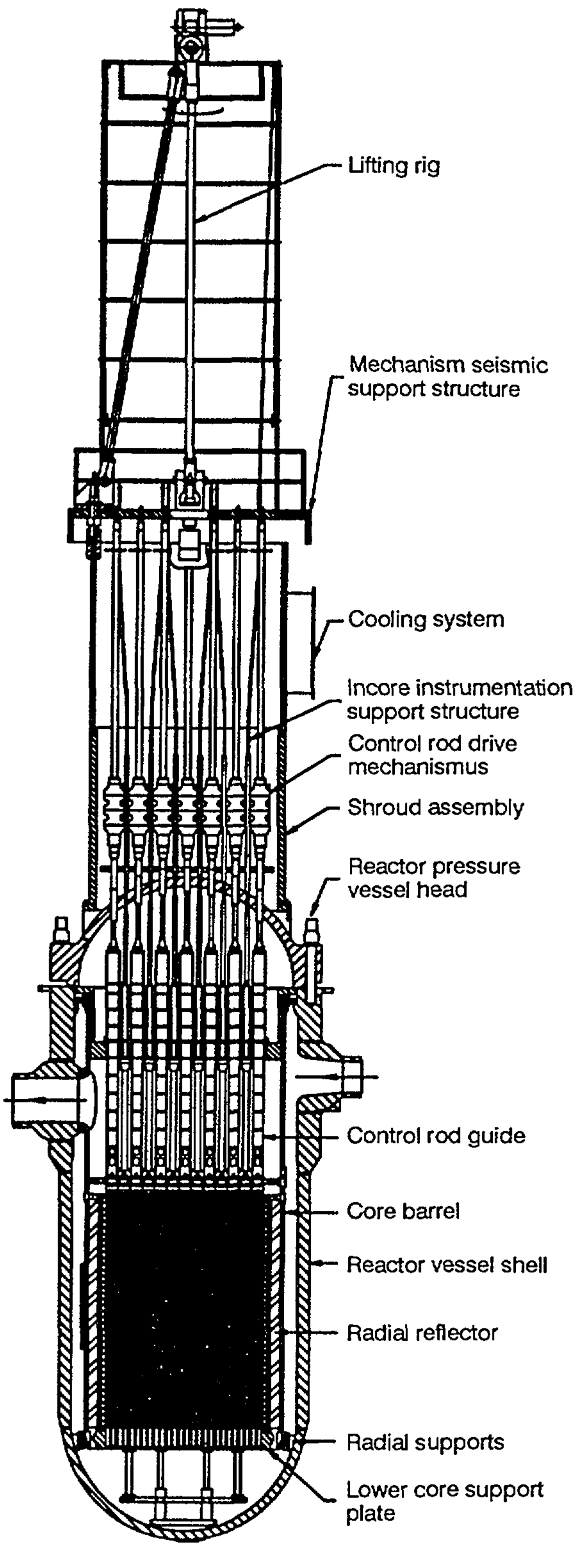


Fig. 1: AP600 reactor system: Proven technology with enhanced performance

channel head of each steam generator. This allows the pumps and steam generator to use the same structural support, greatly simplifying the support system and providing more space for pump and steam generator maintenance. The combined steam generator/pump vertical support is a single pinned column extending from the cell floor to the bottom of the channel head. The steam generator channel head is a one-piece forging with manufacturing and inspection advantages over multipiece, welded components. The integration of the pump suction into the bottom of the steam generator channel head eliminates the crossover leg of coolant loop piping, thus avoiding the potential for core uncovery due to loop seal venting after a small loss-of-coolant accident (LOCA).

The simplified, compact arrangement of the RCS, shown in Figure 2, also provides other benefits. The RCS piping is configured with two main coolant loops. The two cold leg lines of each loop are identical (except for instrumentation and small line connections) and include bends to provide a low-resistance flow path and flexibility to accommodate the expansion difference between the hot and cold leg pipes. The one-piece piping is forged and then bent by a hot induction forming process. The use of a pipe bend reduces costs and in-service inspection requirements by eliminating welds. The loop configuration and material selection yield sufficiently low pipe stresses so that the primary loop and large auxiliary lines meet the requirements to demonstrate leak-before-break. Thus, pipe rupture restraints are not required, greatly simplifying the design and providing good maintenance access. The simplified RCS loop configuration also allows for a significant reduction in the number of snubbers, whip restraints, and supports.

Steam Generator.

The steam generator is based on standard Westinghouse Model F technology. There are currently 84 Model F steam generators operating in 25 nuclear plants with a wide range of operating environments. To date, they have accumulated over 450 steam-generator-years

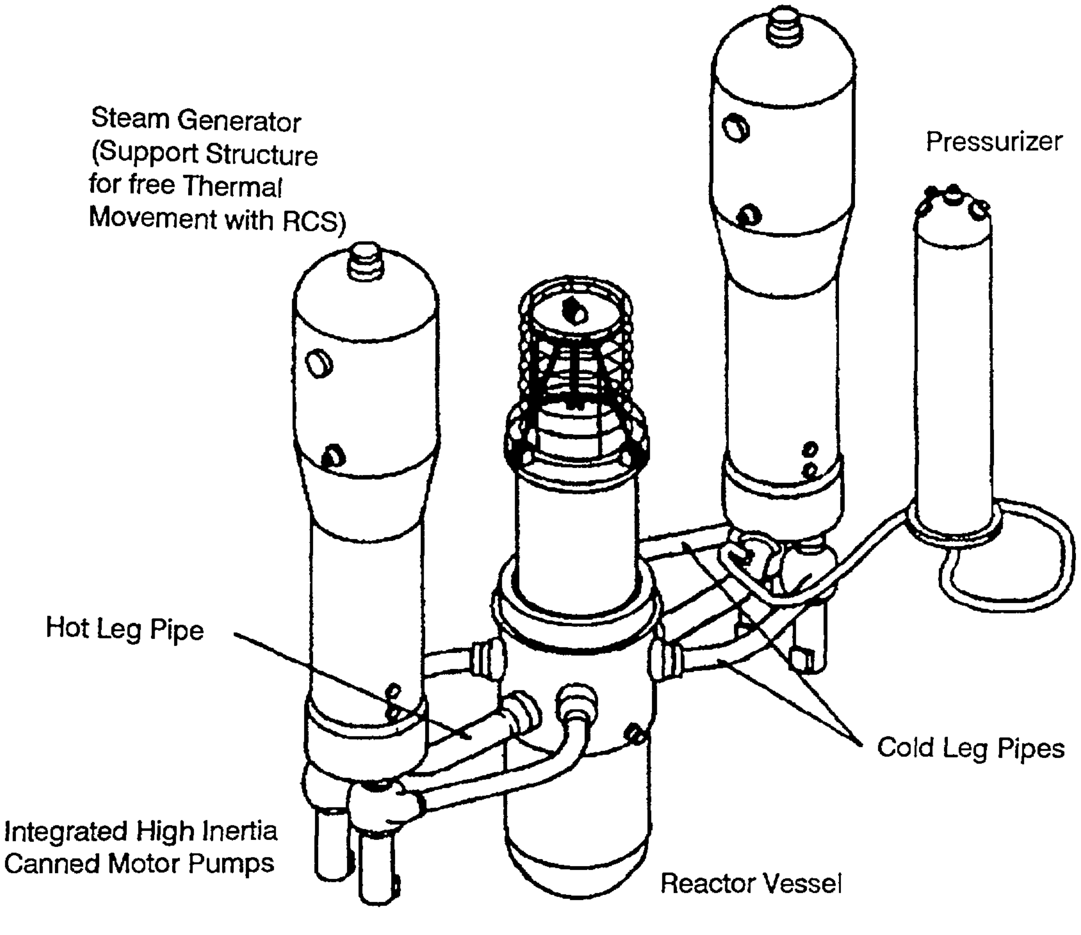

Steam Generator (Support Structure for free Thermal Movement with RCS)
Pressurizer
Hot Leg Pipe
Cold Leg Pipes
Integrated High Inertia Canned Motor Pumps
Reactor Vessel

Fig. 2: RCS loop layout: Proven components in simplified arrangement

of operation with less than one tube plugged per year of operation. The 25 Model F-type replacement steam generators have an even more impressive record with less than one tube plugged per steam generator for every four years of operation. This is the highest level of reliability achieved by any steam generator worldwide. These reliability achievements are due to a variety of design enhancements, including full-depth hydraulic expansion, stainless steel broached tube support plates, and Alloy 690 thermally treated tube material. All the Model F-type steam generators have operated on all volatile treatment secondary side water chemistry. A cutaway drawing of the AP600 steam generator is shown in Figure 3.

Reactor Coolant Pumps.

The reactor coolant pumps are a canned motor design incorporating the latest commercial and marine canned motor pump technology. The canned motor pump is a highly reliable unit used extensively (approximately 1,300 built) in nuclear and fossil applications for over 38 years. Because it has no seals, it does not require a seal water system. Thus, continuous charging pump operation is not required and the chemical and volume control system is simplified.

Since the pumps have no shaft seals, they cannot cause a seal failure LOCA. This is a significant safety enhancement, as seal failure LOCAs are a major industry issue. Maintenance is also enhanced, since seal replacement is unnecessary.

In the AP600 application, the pumps are mounted in the inverted (motor-below-casing) position. Inverted canned motors have been in operation for over 28 years in fossil boiler circulation systems. These pumps have better operating reliability than upright units because the motor cavity is self-venting into the pump casing, avoiding the potential for gas pockets in the bearing and water regions.

One modification of the AP600 pumps from commercial and marine canned motor pump practice is the use of a flywheel to increase the pump rotating inertia. The increased inertia provides a slower rate-of-flow coastdown to improve core thermal margins following the loss of electric power.

Pressurizer.

The pressurizer is of conventional design, based on proven technology and years of operating experience. The pressurizer is about 30 percent larger than that normally used in a plant of comparable power rating. The larger pressurizer increases transient operation margins, resulting in a more reliable plant with fewer reactor trips, and avoiding challenges to the plant and operator during transients. It also eliminates the need for fast-acting power-operated relief valves, which are a possible source of RCS leakage and maintenance.

1.3. Passive safety systems

The use of passive safety systems provides superiority over conventional plant designs through significant and measurable improvements in plant simplification, safety, reliability, and investment protection. The AP600 uses passive safety systems to improve the safety of the plant and to satisfy NRC safety criteria. The passive safety systems require no operator actions for 72 hours to mitigate design basis accidents. These systems use only natural forces such as gravity, natural circulation, and compressed gas to make the systems work. No pumps, fans, diesels, chillers, or other active machinery are used. Simple valve alignment

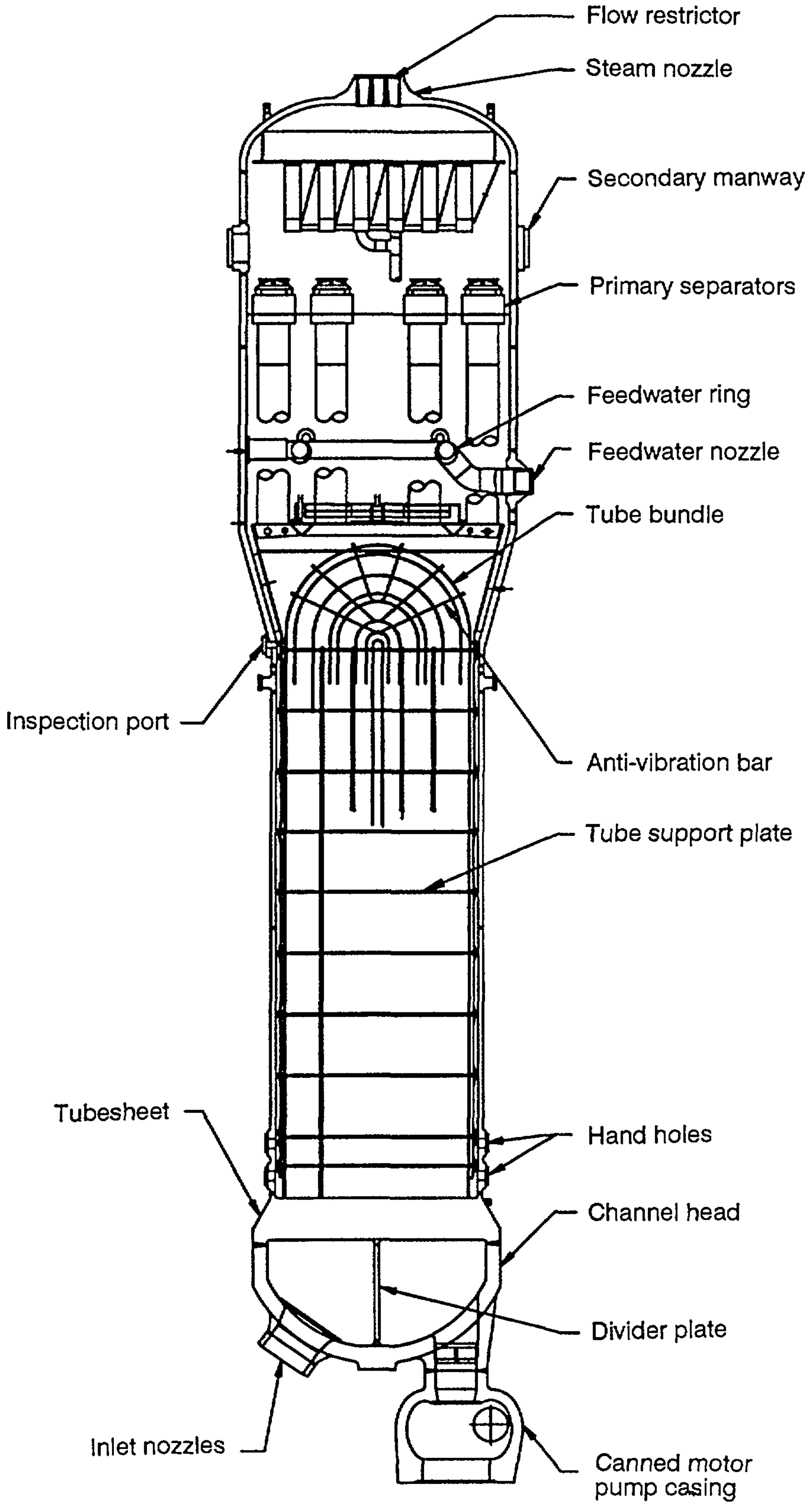


Fig. 3: Improved AP600 steam generator: Based on proven model F design

automatically actuates the passive safety systems. To provide high reliability, these valves are designed to actuate to their safeguards positions upon loss of power or upon receipt of a safeguards actuation signal. However, they are also supported by multiple, reliable power sources to avoid unnecessary actuations.

The AP600 passive safety-related systems include:

- The passive core cooling system (PXS)
- The passive containment cooling system (PCS)
- The main control room habitability system (VES)
- Containment isolation

These passive safety systems provide a major enhancement in plant safety and investment protection as compared with conventional plants. They establish and maintain core cooling and containment integrity indefinitely, with no operator or ac power support requirements. The passive systems are designed to meet the NRC single-failure criteria, and probabilistic risk assessments (PRAs) are used to verify their reliability. These passive safety systems are also designed to satisfy other NRC criteria including Three Mile Island lessons learned, Standard Review Plan, Regulatory Guides, and unresolved and generic safety issues. The performance of the passive safety systems in mitigating design basis events is documented in the Standard Safety Analysis Report (SSAR) and PRA documents submitted to the NRC in mid-1992.

Passive Core Cooling System.

The PXS protects the plant against reactor coolant system (RCS) leaks and ruptures of various sizes and locations. The PXS provides the safety functions of core residual heat removal, safety injection, and depressurization. Safety analyses (using NRC-approved codes) demonstrate the effectiveness of the PXS in protecting the core following various RCS break events. The PXS provides approximately a 400°F (220°C) margin to the maximum peak clad temperature limit for the double-ended rupture of a main reactor coolant pipe.

Safety Injection and Depressurization.

The PXS uses three passive sources of water to maintain core cooling through safety injection. Shown in Figure 4, these injection sources include the core makeup tanks (CMTs), the accumulators, and the in-containment refueling water storage tank (IRWST). These injection sources are directly connected to two nozzles on the reactor vessel so that no injection flow can be spilled for the larger break cases. Table 1 highlights the significant simplification achieved by the AP600 safety injection features.

Residual Heat Removal.

The PXS includes two identical 100-percent capacity passive residual heat removal heat exchangers (PRHR HXs). The PRHR HXs are connected through common inlet and outlet lines to RCS loop 1. The PRHR HXs protect the plant against transients that upset the normal steam generator feedwater and steam systems. The PRHR HXs satisfy the NRC safety criteria for loss of feedwater, feedwater line breaks, and steam line breaks using single failure assumptions approved by NRC safety analysis codes, as documented in the AP600 SSAR. Table 2 indicates the significant simplification of the AP600 residual heat removal function.

Passive Containment Cooling System.

The passive containment cooling system (PCS) provides the safety-related ultimate heat sink for the plant. As demonstrated by computer analyses and extensive test programs, the PCS effectively cools the containment following an accident such that the design pressure is not exceeded and the pressure is rapidly reduced. As shown in Figure 4, the steel containment vessel itself provides the heat transfer surface that removes heat from inside the contain-

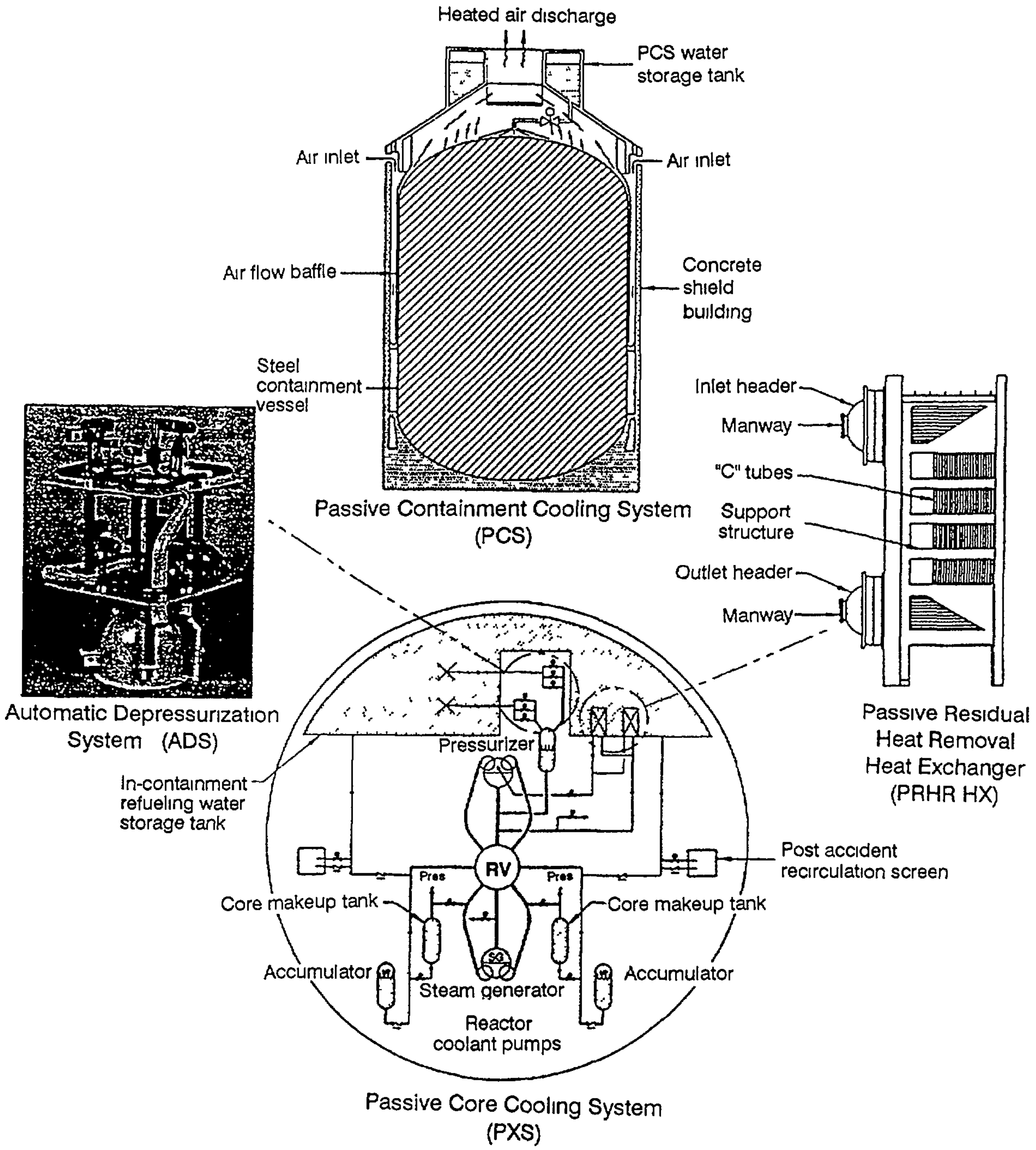


Fig. 4: AP600 passive safety systems: Passive features enhance plant safety, reliability, and availability

TABLE 1 SAFETY INJECTION SIMPLIFICATION: Design reduces piece counts

Component	Conventional 2-Loop Plant	AP600
Pumps	4	0
Tanks	5	5
Remote Valves	85	40

TABLE 2 RESIDUAL HEAT REMOVAL SIMPLIFICATION

Component	Conventional 2-Loop Plant	AP600
Pumps	5	0
Heat Exchangers	2	2
Tanks	1	0
Remote Valves	19	4

ment and rejects it to the atmosphere. Steel containment vessels of similar size have been used on 15 operating PWRs. Heat is removed from the containment vessel by continuous natural circulation flow of air. During an accident, the air cooling is supplemented by evaporation of water. The water drains by gravity from a tank located on top of the containment shield building. Two normally closed fail-open butterfly valves are opened to initiate the water flow. The water tank is sized for 72 hours of operation, after which time the tank is expected to be refilled so that the low containment pressure achieved after the accident (1/4 design pressure in 24 hours) can be maintained. If the water is not resupplied, the containment pressure will increase, but the peak is calculated to reach only 90 percent of design pressure in about two weeks if no operator support actions are taken. Table 3 indicates the large improvement in safety heat sink simplicity resulting from the PCS.

Westinghouse has calculated the AP600 to have a significantly reduced frequency of release of large amounts of radioactivity following a severe accident core damage scenario. This analysis shows that with only the normal PCS air cooling, the containment stays well below the predicted failure pressure. Other factors include improved containment isolation and reduced potential for LOCAs outside of containment. This improved containment performance supports the technical basis for simplification of offsite emergency planning.

Main Control Room Habitability System.

The AP600 main control room habitability system (VES) provides fresh air, cooling, and pressurization to the main control room (MCR) following a plant accident. Operation of the VES is automatically initiated upon receipt of a high MCR radiation signal, which isolates the normal control room ventilation path and initiates pressurization. Following system actuation, all functions are completely passive. Table 4 highlights the simplification achieved by the VES.

Containment Isolation.

AP600 containment isolation is significantly improved over that of conventional PWRs. One major improvement is the large reduction in the number of penetrations. Furthermore, the number of normally open penetrations is reduced by 60 percent. For example, the chemical and volume control system (CVS) letdown penetration is normally closed because the CVS purification occurs in a high-pressure loop, inside containment. Also, there are no penetrations required to support post-accident mitigation functions (the canned motor reactor coolant pumps do not require seal injection, and the residual heat removal and safety injection features are located entirely inside containment). Provided in Table 5 is a summary of the significant AP600 penetration improvements.

Safety Systems Simplification.

A major AP600 plant simplification is the elimination of the traditional safety-related containment spray system. This system is normally required to remove airborne particulates and elemental iodine releases to the containment atmosphere following a core degradation accident in a conventional plant. For the AP600, removal of airborne activity is accomplished by natural processes such as sedimentation and deposition that do not depend on sprays. A summary of the simplification achieved through elimination of the spray system is provided in Table 6.

TABLE 3 SAFETY HEAT SINK SIMPLIFICATION

Component	Conventional 2-Loop Plant	AP600
Pumps	6	0
Tanks/Basins	2	1
Mechanical Draft Cooling Towers	4	0
Remote Valves	34	4

TABLE 4 CONTROL ROOM HABITABILITY SIMPLIFICATION

Component	Conventional 2-Loop Plant	AP600
Safety Fans	4	0
Safety Filters	2	0
Safety Remote Dampers or Valves	8	8

TABLE 5 CONTAINMENT ISOLATION/BYPASS SIMPLIFICATION

Component	Conventional 2-Loop Plant	AP600
Penetrations	93	50
Normally Open Penetrations	38	15

TABLE 6 CONTAINMENT SPRAY SIMPLIFICATION

Component	Conventional 2-Loop Plant	AP600
Pumps	2	0
Tanks	1	0
Remote Valves	8	0

1.4. Defense-In-Depth Systems

The AP600 design provides for multiple levels of defense for accident mitigation (defense-in-depth), resulting in extremely low core damage probabilities while minimizing the occurrences of containment flooding, pressurization, and heat-up situations. This defense-in-depth capability includes multiple levels of defense for a very wide range of plant events. Six separate aspects of the AP600 design contribute to defense-in-depth, as follows:

- A stable, forgiving plant design that accepts mistreatment or anomalies and remains in normal operation.

- Protection against public radiation releases through the various physical plant boundaries.
- Safety-related systems for mitigation functions.
- Diverse mitigation functions within the safety-related systems.
- Additional margin provided by non-safety systems.
- Features to contain anticipated core damage.

Defense-in-Depth Aspects.

This subsection explains each of the six aspects of the AP600 defense-in-depth. Each of these aspects directly contributes to the overall defense-in-depth protection of public safety.

Stable Operation.

In normal operation, the most fundamental level of defense-in-depth ensures that the plant can be operated stably and reliably. This is achieved by the system design features, selection of materials, by quality assurance during design and construction, by well-trained operators, and by an advanced control system and plant design that provide substantial margins for plant operation before approaching safety limits.

Physical Plant Boundaries.

One of the most recognizable aspects of defense-in-depth is the protection of public safety through the physical plant boundaries. Releases of radiation are directly prevented by the fuel cladding, the reactor pressure boundary, and the containment pressure boundary. These boundaries are designed to meet all criteria of 10 CFR 50, Appendix A, and to provide high-integrity public protection against releases of radiation through a strict quality assurance program. In addition, the entire AP600 defense-in-depth structure serves to protect and maintain the integrity of these boundaries. For the fuel cladding boundary, the reactor protection system is designed to actuate a reactor trip whenever necessary to prevent exceeding the fuel design limits. The core design, together with defense-in-depth process and decay heat removal systems, provides this capability under expected conditions of normal operation, with appropriate margin for uncertainties and anticipated transient situations. The reactor coolant pressure boundary is designed with complete overpressure protection and appropriate materials to provide and maintain the boundary during all modes of plant operation. The containment vessel, in conjunction with the defense-in-depth heat removal systems, is designed so that its design pressure is not exceeded following postulated design basis accidents, and containment failure does not occur even under severe accident conditions. The following three defense-in-depth aspects directly support the maintaining of these physical boundaries.

Non-Safety Systems.

The first level of defense-in-depth is the availability of certain non-safety systems for reducing the potential for events leading to core damage. The defense-in-depth non-safety systems are:

- Chemical and Volume Control System (CVS)
- Startup Feedwater System (SFWS)
- Normal Residual Heat Removal System (RNS)
- Spent Fuel Pit Cooling System (SFS)
- Diverse Actuation System (DAS)

For more probable events, these defense-in-depth non-safety systems automatically actuate to provide a first level of defense to reduce the likelihood of unnecessary actuation and operation of the safety-related systems. These non-safety-related systems establish and maintain shutdown conditions for the plant following the more probable events, provided that at least one of the non-safety-related ac power sources is available.

Passive Safety-Related Systems.

The highest level of defense includes the AP600 safety-related passive systems and equipment. The safety-related passive systems, described in Section 3, are sufficient to automatically establish and maintain core cooling and containment integrity for the plant following design basis events, assuming that the most limiting single failure occurs. These systems maintain core cooling and containment integrity after an event, without operator action and onsite and offsite ac power sources, for an indefinite amount of time.

To provide single-failure protection, the passive safety systems are designed with extensive redundancy. An additional level of defense is provided through the diverse mitigation functions within the passive safety-related systems themselves. This diversity exists, for example, in the residual heat removal function. The PRHR HXs are the passive safety-related feature for removing decay heat during a transient. In case of multiple failures in the PRHR HX, defense-in-depth is provided by the passive safety injection and automatic depressurization (passive feed and bleed) functions of the Passive Core Cooling System.

The passive safety systems also contain diversity through the use of physically different components within a system to prevent possible common-cause failures.

Containing Anticipated Core Damage.

As a final level of defense-in-depth, the AP600 has features specifically to contain anticipated core damage. The containment hydrogen control system includes hydrogen recombiners and igniters to limit the hydrogen concentration in containment. The hydrogen concentration is limited so that the containment pressure boundary integrity is not challenged. Operation of the hydrogen recombiners is not required until the hydrogen concentration reaches 3.5 volume percent, which takes six days after the design basis LOCA. Igniters are available for more severe core damage scenarios with higher hydrogen generation rates. Their availability is maintained through simple post-72-hour support actions. Another feature provided to contain core damage is the region of space located below the reactor vessel which is designed specifically to provide adequate debris bed coolability. Futhermore, the in-containment refueling water storage tank is equipped with dump valves to guarantee release of its contents onto the containment floor for cooling the melted core. Finally, the PCS air-only cooling is capable of mitigating core damage scenarios for an unlimited amount of time.

1.5. Advanced instrumentation and control

Advanced, microprocessor-based I&C systems also contribute to overall plant safety by simplifying and enhancing plant operation and maintenance. A digital, multiplexed control system takes the place of hardwired analog controls and cable-spreading rooms, accounting for a significant decrease in control cable (80 percent less control cable than current nuclear plants). I&C components feature built-in diagnostics and board level repair. Most faults can be repaired quickly by swapping a printed circuit card or instrument module. Other AP600 I&C features that enhance safety and reliability are: train separation, self-diagnostics, and equipment monitoring.

Data derived from extensive human-factors studies are used throughout the I&C and control room design to enhance operability and decrease the probability of operator error. These data were also incorporated into the design of the alarms, displays, controls, and procedures; the computer-driven graphics and safety-qualified displays simplify the operators' tasks in assimilating information. The result is a control room design that brings the plant to the operator, rather than making the operator go to the plant.

2 DESCRIPTION OF 15 SPECIFIC DESIGN AREAS AS SELECTED FROM INSAG-3

In the following sections the reference to INSAG-3 is put in parentheses after each heading.

2.1. Plant process control systems (4.2.2.1)

Normal Operation and anticipated operational occurrences are controlled so that the plant and system variables remain within their operating ranges. This reduces the frequency of demands on the safety systems.

The AP600 is designed to withstand the following operational occurrences without the generation of a reactor trip or actuation of the safety related passive engineered safety systems:

- ± 5%/minute ramp load change within 15% and 100% power
- ± 10% step load change within 15% and 100% power
- 100% generator load rejection
- 100-50-100% power level daily load follow over 90% of the fuel cycle life
- Grid frequency changes equivalent to 10% peak-to-peak power changes at 2%/minute rate
- 20% power step increase or decrease within 10 minutes
- Loss of a single feedwater pump

The logic and setpoints for all of the AP600 Nuclear Steam Supply System (NSSS) control systems are developed in order to meet the above operational transients without reaching any of the protection system setpoints.

Reactor power oscillations are inherently damped by the incorporation of a negative Doppler coefficient and nonpositive moderator temperature coefficients of reactivity. The control system logic and setpoints are developed to mitigate the possibility of short-term and long-term oscillations around the desired reactor coolant system temperature setpoint.

The NSSS control systems (rod control, pressurizer pressure and level control, steam generator level control, steam dump control, and required inputs from the turbine/generator) use inputs from various transmitters. The control systems use redundant inputs in order to prevent the control system from responding in an adverse manner to a single failure of an input signal or transmitter.

For reactivity control two separate means are provided. For short term response to operational transients, rod cluster control assemblies are used. Two different sets are provided, each with their own separate control system logic. The first set controls gross thermal power inserting or withdrawing control rods in demand to changes in RCS temperature. The second set of RCCAs is designed to adjust the axial power distribution during day to night load cycling maneuvers. A separate control system regulates the position of these control rods. For long term countering of core burnup, a chemical shim control is used. The combined use of control rod and gray rod assemblies, and the chemical shim control system permits the necessary shutdown margin to be maintained following a reactor trip.

1.2. Automatic safety systems (4.2.2.2)

Automatic safety systems are provided that would safely shut down the reactor, maintain it in a cooled state, and limit any radioactive release that might possibly ensue, if operating conditions were to exceed predetermined setpoints.

The plant protection system, a microprocessor based system, trips the reactor and actuates engineered safety features when predetermined limits are exceeded or when manually initiated. The reactor trip portion of the protection system includes four independent, redundant, physically separated, electrically-isolated channels. The coincidence circuits guard against the loss of protection or the generation of false protection signals due to equipment failures through use of a two-out-of-four logic and built-in operational bypasses.

The automatic safety system which maintains the reactor in a cooled state is the Passive Core Cooling System, designed to perform the following:

- Emergency Reactor Coolant System (RCS) Makeup and Boration during transients or accidents when the normal RCS makeup from the Chemical and Volume Control is lost or insufficient.
- Safety Injection is provided to the RCS to enure adequate core cooling for the complete range of LOCAs up to and including the double ended rupture of the largest RCS piping.
- Emergency Core Decay Heat Removal is provided during transients, accidents, or whenever the normal heat removal paths are lost. This heat removal function must be available for all RCS conditions, including plant shutdown and refuelling.

The safety grade ultimate heat sink for the removal of RCS sensible heat and core decay heat is the function of the Passive Containment Cooling System (PCS). The PCS has the capability to remove sufficient energy form the reactor containment structure to prevent the containment from exceeding its design pressure and to reduce containment pressure following design basis events.

2.3. Protection against power transient accidents (4.2.3.1)

The AP600 is designed so that reactivity induced accidents are protected against, with a conservative margin of safety, by inherent negative reactivity feedback and by automatic systems which introduce neutron absorbers.

When the reactor is critical, the negative fuel temperature reactivity effects (Doppler feedback) provides prompt reactivity feedback to compensate for a rapid, uncontrolled reactivity excursion. The negative doppler coefficient of reactivity is provided by the use of low-enrichment fuel design. For slower reactivity transients that result in moderator temperature increases, the non-positive moderator temperature coefficient of reactivity provides compensatory reactivity feedback.

The AP600 uses two methods to introduce neutron absorbers for reactivity control: rod cluster control assemblies (RCCA) and chemical shim (boric acid). The rod cluster control assemblies are arranged in banks some of which are used in normal plant control and others which are used for shutdown. During operation, the shutdown rod banks are fully withdrawn, however, during an accident, they are inserted into the core by the force of gravity.

The shutdown and control rod banks provide reactivity margin to shut down the reactor during normal operating conditions and during anticipated operational occurrences, without exceeding specified fuel design limits. The plant is provided with the means of holding the core subcritical under any anticipated conditions with appropriate margin. The combined use of the control rod assemblies and the chemical shim control system permits the necessary shutdown margin to be maintained during long-term xenon decay and plant cooldown. The single highest worth control rod assembly is conservatively assumed to be stuck in the fully withdrawn position for this determination.

2.4. Reactor core integrity (4.2.3.2)

The core is designed to have mechanical stability. It is designed to tolerate an appropriate range of anticipated variations in operational parameters. The core design is such that the expected core distortion or movement during an accident within the design basis would not impair the effectiveness of the reactivity control or the safety shutdown systems or prevent cooling of the fuel.

<u>Measures Incorporated in the AP600:</u>

For design purposes, the AP600 plant conditions are divided into four categories.

- Condition I - normal operation and operational transients
- Condition II - events of moderate frequency
- Condition III - infrequent incidents
- Condition IV - limiting faults

The reactor is designed so that its components meet the following performance and safety criteria:

- Fuel damage (i.e., breach of fuel rod cladding) is not expected during Condition I and Condition II events. A very small amount of fuel damage may occur. This is within the capability of the plant cleanup system and is consistent with plant design bases.

- The reactor can be brought to a safe state following a Condition III event with only a small fraction of fuel rods damaged. The fraction of fuel rods damaged must be limited to meet the dose guidelines of 10CFR100 although sufficient fuel damage might occur to preclude immediate resumption of operation.

- The reactor can be brought to a safe state and the core kept subcritical with acceptable heat transfer geometry following Condition IV events.

The fuel rods are designed to satisfy the fuel rod design criteria for rod burnup levels up to the design discharge burnup. The AP600 fuel rod design considers effects such as fuel density changes, fission gas release, clad creep, and other physical properties which vary with burnup. The integrity of the fuel rods is provided by designing to prevent excessive fuel temperatures, excessive internal rod gas pressures due to fission gas releases, and excessive cladding stresses, strains, and strain fatigue.

Fuel Assembly Structural Design

Normal Operation (Condition I) and Upset (Condition II)

The fuel assembly component structural design criteria are established for the two primary material categories, austenitic steels and zirconium alloys. The stress categories and strength theory presented in the ASME Code, Section III, are used as a general guide.

The volume average effective clad stress calculated with the Von Mises equation (considering interference due to uniform cylindrical pellet-clad contact, caused by pellet thermal expansion, pellet swelling and uniform clad creep, and pressure differences) is less than the 0.2 percent offset yield stress with due consideration to temperature and irradiation effects for Condition I and II events. While the clad has some capability for accommodating plastic strain, the yield stress has been accepted as a conservative design limit.

The total plastic tensile creep strain de to uniform clad creep, and uniform cylindrical fuel pellet expansion associated with fuel swelling and thermal expansion is less than one percent from the unirradiated condition. The rod internal gas pressure remains below the value which causes the fuel/clad diametral gap to increase due to outward cladding creep during steady-state operation. The acceptance limit for fuel rod clad strain during Condition II events is that the total tensile strain due to uniform cylindrical pellet thermal expansion is less than one percent from the pre-transient value. These limits are consistent with proven practice.

The effect of flow-induced vibration on the fuel assembly and individual fuel rods is minimal. The cyclic stress range associated with deflections of such small magnitude is insignificant and has no effect on the structural integrity of the fuel rod. The reaction force on the grid supports, due to rod vibration motions, is also small and is much less than the spring preload. Adequate fuel clad spring contact is maintained. No significant wear of the clad or grid supports is predicted during the life of the fuel assembly based on out-of-pile flow tests, performance of similarly designed fuel in operating reactors, and design analyses.

The usage factor due to cyclic fatigue is less than 1.0. That is, for a given strain range, the number of strain fatigue cycles are less than those required for failure. The fatigue curve is based on a safety factor of two on the stress amplitude or a safety factor of 20 on the number of cycles, whichever is more conservative.

Infrequent Incidents (Condition III) and Limiting Faults (Condition IV)

Typical worse case abnormal loads during Conditions III and IV are represented by seismic and pipe rupture loadings. The criteria for this category of loadings are:

- Deflections or excessive deformation of components cannot interfere with capability of insertion of the control rods or emergency cooling of the fuel rods.
- The fuel assembly structural component stresses under faulted conditions are evaluated primarily using the methods outlined in Appendix F of the ASME Code, Section III.

To demonstrate that the fuel assemblies will maintain a coolable geometry under the worst-case accident Condition IV event, a plant specific or bounding seismic analysis is performed. The fuel assembly response resulting from safe shutdown earthquake condition is analyzed using time-history numerical techniques. The motions of the reactor internals upper and lower core plates and the core barrel at the upper core plate elevation, which are simultaneously applied to simulate the reactor core input motion, are obtained from the time-history analysis of the reactor vessel and internals. The fuel assembly response, namely the displacements and impact forces, is obtained with the reactor core model. Similar dynamic analyses of the core were performed using reactor internals motions indicative of the postulated pipe rupture. Scenarios regarding breaches in the pressure boundary are investigated to determine the most limiting structural loads for the fuel assembly.

Grid component strength criteria are based on experimental tests. The limit is established at the 95-percent confidence level on the true mean crush strength at operating temperature. This limit ensures that the core will maintain a coolable geometry under the worst-case combined seismic and pipe rupture event.

The stresses induced in the various fuel assembly nongrid components are assessed based on the most limiting seismic condition. The fuel assembly axial forces resulting from the hold-down spring load together with its own weight distribution are the primary sources of the stresses in the guide thimbles and fuel assembly nozzles. The fuel rod accident induced stresses, which are generally very small, are caused by bending due to the fuel assembly deflections during a seismic event. The seismic-induced stresses are compared with the allowable stress limits for the fuel assembly major components. The stresses are below the established allowable component limits. Consequently, the structural designs of the fuel assembly components are acceptable for the design basis accident conditions.

2.5. Automatic shutdown systems (4.2.3.3)

Rapidly responding and highly reliable reactivity reduction for safety purposes is designed to be independent of the equipment and processes used to control the reactor power. Safety shutdown action is available at all times when steps to achieve a self-sustaining chain reaction are being intentionally taken or whenever a chain reaction might be initiated accidentally.

Reactor trip is a protective function performed by the integrated protection system when it anticipates an approach of a parameter to its safety limit. Reactor shutdown occurs when electrical power is removed from the rod drive mechanism coils, allowing the rods to fall by gravity into the reactor core.

The protection system maintains surveillance of key process variables directly related to equipment mechanical limitations (such as pressure), and of variables which directly affect the heat transfer capability of the reactor (such as flow and temperature). Four redundant measurements using four separate sensors are made for each variable used for reactor trip. A partial trip signal for a parameter is generated if one channel's measurement exceeds its predetermined or calculated limit. Each division sends its partial trip status to each of the other three divisions over isolated multiplexed data links. Each division is capable of generating a reactor trip signal if two or more of the redundant channels of a single variable are in the partial trip state.

The reactor trips are:

Source Range Reactor Trip
Intermediate Range Reactor Trip
Power Range (low setpoint or high setpoint) Trip
High Positive Flux Rate Trip
Overtemperature Delta T
Overpower Delta T
Pressurizer Low Pressure/ High Pressure Trip
Pressurizer High Water Level Trip
Low Reactor Coolant Flow
Reactor Coolant Pump Underspeed
Low or High Steam Generator Water Level
Automatic Safeguards Actuation
Automatic Depressurization System Actuation
Manual Safeguards Actuation
Manual Reactor Trip

2.6. Normal heat removal (4.2.3.4)

The reactor coolant system (RCS) is the primary heat removal safety system used to cool the core by transferring the heat produced in the core to the secondary side of the plant. It consists of two heat transfer circuits, each with a steam generator (channel head and tubes), two reactor coolant pumps, and a single hot leg and two cold legs. The RCS performs this function during normal power (1-100%) operation as well as when the reactor is subcritical, including the initial phase of plant cooldown. The RCS is also the preferred means of shutdown and decay heat removal after most accidents. This is accomplished by forced circulation with the reactor coolant pumps operating or by natural circulation if the pumps do not operate.

The normal residual heat removal system provides secondary means of cooling the core by transferring both residual and sensible heat from the core via the RCS during the second phase of plant cooldown.

Following cooldown, the normal residual heat removal system is the normal pathway to remove heat from the core and the RCS during the entire plant shutdown, until the plant is started again. The normal heat removal system is not a safety system. It is not required to operate to mitigate design basis accidents. Passive core cooling features remain available during shutdown to provide the safety-related function of core cooling for accident scenarios.

2.7. Emergency heat removal (4.2.3.5)

Provision is made for alternate means to restore and maintain fuel cooling under accident conditions, even if normal heat removal fails or the integrity of the primary cooling system boundary is lost.

The AP600 design provides for safety-related passive reactor coolant makeup. Core makeup tanks accommodate small leaks when the normal makeup system is unavailable and provide safety injection for small-break loss of coolant accidents (LOCA). Accumulators provide the high makeup flow required for a large LOCA and initiate injection when the reactor coolant system pressure is below the static accumulator pressure during a LOCA. The in-containment refuelling water storage tank, and after containment flood-up, the containment recirculation sump provides the long-term source of gravity injection to the core after the RCS is depressurized. The automatic depressurization system valves provide the vent path to transfer the core decay heat to the containment and then to the ultimate heat sink. The AP600 design provides a passive core cooling system that functions during at-power and shutdown conditions until the refuelling cavity is capable of providing core cooling.

For events not involving a loss of coolant, emergency core decay heat removal is provided by the passive core cooling system via the passive residual heat removal heat exchangers. The heat exchangers are located in the in-containment refueling water storage tank, which provides the heat sink for the heat exchangers, in conjunction with the operation of the passive containment cooling system. The passive residual heat removal heat exchangers are elevated above the reactor coolant system loops to induce natural circulation flow through the heat exchangers when the reactor coolant pumps are not available. The passive core cooling system functions independent of ac power supplies. The passive core cooling system does not need the non-safety-related diesel-generators for electrical power to either actuate or operate the various system components. Therefore, the passive core cooling system complies with the intent of GDC 35 by providing the capability for core cooling without relying on non-safety-related ac power sources.

The AP600 design uses passive systems for long-term post-loss of coolant accident core and containment heat removal and for the prevention of gradual overpressurization failure of the containment building. Heat is transferred from the interior to the steel containment shell by natural convection. Heat removal from the exterior of the containment shell is enhanced by a directed-flow natural convection design and a passive, external cooling system. The AP600 passive containment cooling system is designed with sufficient capacity to prevent the containment from exceeding its design pressure with no operator action or outside assistance. The AP600 passive containment cooling system consists of a steel containment shell and associated water supplies, piping, valves, and air baffle. The passive containment cooling system is a passive system that uses gravity and natural circulation as driving forces. The design of the AP600 passive containment cooling system does not require the use of any pumps, and it functions independent of nonsafety-related ac power sources. Therefore, the passive containment cooling system can function during loss of offsite or onsite power. GDC

38 is satisfied by using appropriate redundancy and by the design of the passive containment cooling system and its reliance on natural forces.

2.8. Reactor coolant system integrity (4.2.3.6)

Codes and standards for nuclear vessels and piping are supplemented by additional measures to prevent conditions arising that could lead to a rupture of the primary coolant system boundary at any time during the operational life of the plant.

Structures, systems, and components in the AP600 are classified according to nuclear safety classification, quality groups, and seismic categories. The AP600 classification system provides an easily recognizable means of identifying the extent to which structures, systems, and components, are related to ANS nuclear safety classification, NRC quality groups, ASME Code classification, seismic category and other applicable industry standards. Components of the AP600 Reactor Coolant Pressure Boundary (RCPB) are designed as Safety Class A, the highest quality standard in accordance with General Design Criterion 30.

The following summarizes specific AP600 design features and requirements relevant to the IAEA Safety Principles.

Component Design, Materials and Fabrication

The AP600 RCPB components are designed to the requirements of ASME Section III, Subsection NB (Class 1 components), with component supports designed to Subsection NF. Base metals and welding materials conform to the applicable ASME Code Material Specifications. In addition, numerous supplemental requirements are implemented, to avoid material degradation from causes such as intergranular attack, stress corrosion cracking, thermal and mechanical fatigue, radiation effects, welding related failures, bolting failures and casting flaws. These requirements are consistent with the ALWR Utility Requirements Document. Examples of these supplemental requirements include:

- Requirements to improve resistance to stress corrosion cracking of austenitic stainless steel, including limits on carbon content, requirements for solution heat treatment, control of ferrite content and hardness. Applications requiring the special properties of a nickel based alloy (steam generator tubing, reactor vessel head penetrations) utilize thermally treated nickel-chromium-iron Alloy 690.
- Leak Before Break (LBB) criteria and analysis methodology is applied to most the primary piping. LBB methodology places strict limits on calculated stresses and on material fracture toughness properties. It also requires thorough evaluation of pipe degradation mechanisms including erosion-corrosion induced wall thinning, stress corrosion cracking, water hammer, fatigue, thermal aging and thermal stratification.

Inspection

Inspectability reviews are conducted on components and piping, to ensure that access provisions and component geometry allow inspection. Inspectability is enhanced by use of forged materials in preference to castings for RCPB components except the reactor coolant pump casing. Material requirements are also implemented to improve inspectability, including controls on grain size and uniformity, surface finish, etc.

Overpressure Protection

Reactor coolant system overpressure protection during power operation is provided by the pressurizer safety valves, in conjunction with the reactor protection system. These systems provide compliance with the overpressure protection requirements of ASME Section III. Low temperature overpressure protection is provided by a relief valve on the suction line of the normal residual heat removal system.

Fracture Toughness

Westinghouse has conducted a test program to determine the fracture toughness of low-alloy ferritic materials with specified minimum yield strengths greater than 50,000 psi (345 MPa). In this program, fracture toughness properties were determined and shown to be adequate for base metal plates and forgings, weld metal, and heat-affected zone metal for higher-strength ferritic materials used for components of the reactor coolant pressure boundary.

Beyond the regulatory requirements, fracture toughness is also addressed by means of strict limits on material chemistry, especially copper and phosphorus in the reactor vessel beltline region. In addition, end-of-life neutron fluence on the AP600 reactor vessel has been reduced by the combination of a large vessel diameter, low power density core and a radial reflector. The vessel is fabricated from ring forgings to eliminate longitudinal welds, and the circumferential welds are located outside the beltline region. Limitations have been placed on initial nil ductility temperature and calculated end-of-life RT_{ndt} shift, consistent with the ALWR Utility Requirements Document.

Reactor Vessel Materials Surveillance Monitoring

The AP600 includes a material surveillance program to monitor reactor vessel irradiation and its effect on material properties.

Reactor Coolant Pressure Boundary Leak Detection

The AP600 includes a means to detect and, to the extent practical, identify the source of RCPB leakage of greater than 0.5 gallons per minute (1.9 l/min).

2.9. Confinement of radioactive material (4.2.3.7)

The plant is designed to be capable of retaining the bulk of the radioactive material that might be released from fuel, for the entire range of accidents considered in the design.

The AP600 containment components are designed to the requirements of ASME Boiler and Pressure Vessel Code, Section III. The containment vessel is designed and constructed according to ASME Code, Section III, Subsection NE, Metal Containment. The Containment Isolation System is designed to the ASME Code Section III Class 2 requirements.

The containment system is designed such that for all break sizes, up to and including the double-ended severance of a reactor coolant pipe or secondary pipe, the containment peak pressure is below the design pressure. The passive containment cooling system provides heat transfer from the steel containment to the environment, thus preventing the containment from exceeding design pressure and temperature.

The containment isolation system allows normal or emergency passage of fluids through the containment boundary while preserving the integrity of the containment boundary, if required. Containment isolation provisions are designed so that fluid lines which penetrate the primary containment boundary are isolated in the event of an accident to minimize the release of radioactivity to the environment. Piping systems penetrating the containment have containment isolation features. These features serve to minimize the release of fission products following a design basis accident. Lines that penetrate the containment that are either part of the RC pressure boundary or connect directly to the containment atmosphere, or, satisfy the requirements for a closed system are provided with containment isolation valves.

In addition to the regulatory requirements, the AP600 containment system is designed to comply with the following additional requirements.

- The number of pipe lines which provide a direct connection between the inside and outside of primary containment during normal operation are minimized.
- Closed systems outside of containment that may be open to the containment atmosphere during an accident are designed for the same conditions as the containment itself, and are testable during Type A leak tests.
- The total number of penetrations requiring isolation valves are minimized by appropriate system design.
- Penetration lines with automatic isolation valves are isolated by engineered safety features actuation signals.
- Isolation valves are designed to have the capacity to close against the conditions that may exist during events requiring containment isolation.
- Normally closed manual containment isolation valves have provisions for locking the valves closed. Locking devices are designed such that the valves can be locked only in the fully closed position.
- Automatic containment isolation valves are powered by Class 1E dc power. Non-motor-operated valves fail in the closed position upon loss of a support system, such as instrument air or electric power.

2.10. Protection of confinement structure (4.2.3.8)

The AP600 is designed to withstand the effects of earthquakes without the loss of capability to perform its safety functions. Seismic design is based on the safe shutdown earthquake (SSE). The peak ground acceleration of the safe shutdown earthquake has been established as 0.30g. The vertical peak ground acceleration is conservatively assumed to equal the horizontal value of 0.30g. The operating base earthquake (OBE) has been eliminated as a design requirement for the AP600.

General Design criterion 2 requires that nuclear power plant "Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena, such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions". The seismic classification methodology used in AP600 is consistent with this. Seismic Category I applies to both functionality and integrity. The nuclear Island which includes the basemat, containment interior, shield building, auxiliary building and containment air baffle; and the Containment vessel are classified as Seismic Category I.

Wind loadings for Seismic Category I structures is specified as a basic wind speed of 110 mph (49 m/s) with an annual probability of occurrence of 0.02. This wind speed is the fastest wind speed at 33 feet (10 m) above the ground in open terrain. Higher winds with a probability of occurrence of 0.01 are used in the design of Seismic Category I structures by using an importance factor of 1.11.

Seismic Category I structures are designed to resist tornado loads without exceeding the allowable stresses. Seismic Category I structures are permitted to sustain local missile damage such as partial penetration and local cracking or permanent deformation or both.

The design parameters applicable to the design basis tornado are:
Maximum wind speed - 300 mph (134 m/s)
Maximum rotational speed - 240 mph (107 m/s)
Maximum Transitional speed - 60 mph (27 m/s)
Radius of max. rotational wind from center of tornado - 150 ft (46 m)
Atmospheric pressure drop - 2.0 psi (13.8 kPa)
Rate of pressure change - 1.2 psi/sec (8.3 kPa/s)

Missiles generated by natural phenomena are defined as:

- 4000-pound (1815kg) automobile impacting structure with horizontal velocity of 105 mph (47 m/s) or vertical velocity of 74 mph (33 m/s)
- a 275-pound (125kg), eight inch armor piercing artillery shell impacting the structure with a horizontal velocity of 105 mph (47 m/s) or a vertical velocity of 74 mph (33 m/s)
- a one inch diameter solid steel shell assumed to impinge upon open barrier openings in the most damaging direction at a velocity of 105 mph (47 m/s).

Aircraft Hazards

Aircraft hazards are not addressed in the design basis of U.S. licensing process, rather they are listed in an applicant's Combined License application as a site specific hazard, if applicable.

Containment Protection Against Internal Pressure

The AP600 core damage frequency is calculated to be 3×10^{-7} events per year. The PRA shows that there is no containment failure due to hydrogen burns or other energetic phenomena. The integrated sever accident containment analysis shows that the AP600 containment is capable of performing its function as the ultimate fission product barrier, and no containment failures occur from containment overpressure or over temperature.

2.11. Monitoring of plant safety status (4.2.3.9)

Parameters to be monitored in the control room are selected, and their displays are arranged, to ensure that operators have clear and unambiguous indications of the status of plant conditions important to safety, especially for the purpose of identifying and diagnosing the automatic actuation and operation of a safety system or the degradation of defense in depth.

Instrumentation and controls are provided to monitor and control neutron flux, control rod position, fluid temperatures, pressures, flows, and levels and necessary, to maintain plant safety. The safety related indications that are required for operator use under normal operating and accident conditions are displayed on the Safety-Related Display Information System.

The main control area is designed to support AP600 operator reliability by providing well designed working arrangement of the human engineered resources for the operating staff to monitor and control the plant processes. The main control area contains the following major pieces of equipment, each designed based on the M-MIS design process:

- wall panel information station
- work positions A and B
- supervisor's work position
- safety panel with dedicated controls

The wall panel information provides dynamic display of plant parameters and alarm information so that a high level of understanding of current plant status can be readily ascertained. It is located such that both operators and shift supervisor view it while seated at their work positions.

Work positions A and B contain the displays to start up the plant, maneuver the plant, obtain full-power operation and shut down the plant. The components housed in the work positions are visual display units (seismic and non-seismic), control display units (seismically qualified), plant communication equipment, screen selector controls, component selector controls, and keyboard. The types of information screens available to the operators are functional displays, physical mimic displays, procedure displays, alarm support displays, and special purpose displays.

The safety panel is located between work positions A and B. The qualified plant information system video display units and the dedicated safety system controls are provided in this panel. These monitoring display devices are seismically qualified and provide post-accident monitoring of nuclear reactor safety parameters, including plant process parameters important to safety and the monitoring of effluent paths and plant environs for radioactivity, in accordance with Regulatory Guide 1.97. Analysis has been conducted to identify the appropriate variables and to establish the appropriate design basis and qualification criteria for instrumentation used by the operator for monitoring conditions in the reactor coolant system, the secondary heat removal system, the containment and the system used for attaining a safe shutdown condition.

The main control room also contains monitoring equipment used for fire protection, radiation monitoring, environmental monitoring, and seismic monitoring.

2.12. Preservation of control capability (4.2.3.10)

The control room is designed to remain habitable under normal operating conditions, anticipated abnormal occurrences and accidents considered in the design. Independent monitoring and the essential capability for control needed to maintain ultimate cooling, shutdown and confinement are provided remote from the main control room for circumstances in which the main control room may be uninhabitable or damaged.

The AP600 safety-related control room habitability components are designed to the requirements of ASME Boiler and Pressure Vessel Code, Section III Class 3 requirements.

The habitability systems is defined as a set of individual systems that collectively provide the habitability functions for the plant. The systems that make up the habitability systems are:

- Nuclear island non-radioactive ventilation system
- Main control room emergency habitability system
- Radiation monitoring system
- Fire-smoke detection and alarm systems
- Fire protection system
- Plant lighting system

When ac power is available, the nuclear island non-radioactive ventilation system provides normal and abnormal HVAC service to the main control room (MCR). When a source of ac power is not available to operate the nuclear island non-radioactive ventilation system, the main control room emergency habitability system is capable of providing emergency ventilation and pressurization for the MCR. The main control room emergency habitability system also provides emergency passive heat sinks for the MCR.

The main control room emergency habitability system is made up of two completely redundant trains of Emergency Air Storage Tanks. Each train consists of tanks sized to deliver the required air flow to the MCR to meet the ventilation and pressurization requirements for at least 72 hours.

The main control room emergency habitability system incorporates passive heat sinks for the MCR designed to limit the temperature rise during the 72 hour period following a loss of nuclear island non-radioactive ventilation system operation. The heat sinks primarily consist of the thermal mass of the concrete that makes up the ceilings and walls of these rooms and features to facilitate heat transfer from the room air to the concrete. If cooling of MCR is required beyond 72 hours, portable spot cooling units will be brought in from offsite.

The radiation exposure of MCR personnel throughout the duration of any one of the postulated limiting faults does not exceed the limits set by 10 CFR 50, Appendix A, General Design Criterion 19.

The habitability systems provide the capability to detect and protect MCR personnel from external fire, smoke, and airborne radioactivity. Respiratory, eye, and skin protection is provided for emergency use within the MCR envelope. Toxic gases, including chlorine, are not stored on-site.

Automatic actuation of the individual systems that perform a habitability systems function is provided. Smoke detectors, radiation detectors, and associated control equipment are installed at various plant locations as necessary to provide the appropriate operation of the systems.

If temporary evacuation of the main control room is required because of some abnormal main control room condition, the operators can establish and maintain safe shutdown conditions for the plant from outside the main control room through the use of controls and monitoring located at the remote shutdown station. This station is designed to allow control of a shutdown following an evacuation of the control room, coincident with the loss of offsite power and a single active failure. No other design basis event is postulated. The remote shutdown station equipment is similar to the operator work positions in the main control room and is designed to the same standards.

One remote shutdown station is provided for the plant. The remote shutdown station contains controls for the safety-related equipment required to establish and maintain safe shutdown. Additionally, control of non-safety-related components is available, allowing operation and control when ac power is available. The remote shutdown station also includes a qualified display processing system indication panel identical to the main control room.

2.13. Station blackout (4.2.3.11)

The AP600 is designed such that the simultaneous loss of normal on-site and off-site AC electrical power (a station blackout) will not lead to fuel damage.

The passive plant concept addresses plant safety during station blackout conditions without any need to rely upon ac power sources. The following AP600 design addresses safety issues that could be caused by a loss of offsite and onsite ac power supplies:

- Adequate reactor core protection to prevent offsite radiation dose releases,
- Reliable Class 1E onsite dc power supplies for performance of required safety functions,
- Maintenance of the plant in a safe condition for a minimum of 72 hours during station blackout,
- Safety-grade decay heat removal capability for the duration of a station blackout event,
- Means of reactor coolant system depressurization independent of ac power.

A reliable dc power source supplied by batteries provides power for the safety-related valves and instrumentation during transient and accident conditions. In order to obtain the full benefits of the inherently high reliability and availability of the passive safety systems, sufficient redundancy and backup features are incorporated in the design of the AP600 passive plant dc system to ensure a similar level of reliability of dc power supply and to virtually eliminate any impact of testing and maintenance of the batteries on the operability of the systems.

The Class 1E dc and Uninterruptible Power System (UPS) is the only safety-related power source required to monitor and actuate the safety-related passive systems. Otherwise the plant is designed to maintain core cooling and containment integrity, independent of non-safety-related ac power sources indefinitely. The Class 1E batteries are sized to power dc safety loads on the dc buses and ac safety loads on the associated inverters for a period of 72 hours following Design Bases Event, with all onsite and offsite ac power lost. Although the AP600 is designed with reliable non-safety-related offsite and onsite ac power that are normally expected to be available for important plant functions, non-safety-related ac power is not relied upon to maintain the core cooling or containment integrity.

The non-safety-related ac power system is designed such that the plant auxiliaries can be powered from the grid under all modes of operation. During loss of offsite power, the ac power is supplied by the onsite standby diesel-generators. Preassigned loads and equipment are automatically loaded on the diesel-generators in a predetermined sequence. The onsite standby power system is not required for safe shutdown of the plant.

Provision is made for two non-Class 1E transportable ac generators to meet the post 72 hr power requirements following a highly improbable event of extended loss of all ac sources. The transportable ac generators are designed to be stored at a location far enough from the site so that they remain unaffected by special events such as earthquake, and explosions but close enough to be able to transport them to site within 72 hours.

2.14. Control of accidents within the design basis (4.2.3.12)

Provisions are made at the design stage for the control of accidents within the design basis, including the specification of information and instrumentation needed by the plant staff for following and intervening in the course of accidents.

The plant safety analyses and evaluations define the design basis accident (DBA) event scenarios for which preplanned operator actions are required. Accident monitoring instrumentation is necessary to permit the operator to take required actions to address these analyzed situations. Instrumentation is also necessary for unforeseen situations (should plant conditions evolve differently than predicted by the safety analyses, the control room operating staff has sufficient information to evaluate and monitor the course of the event). Additional instrumentation is also needed to indicate to the operating staff whether the integrity of the fuel cladding, the reactor coolant pressure boundary, or the reactor containment has degraded beyond the prescribed limits defined in the plant safety analyses and other evaluations.

Six types of variables are classified to provide this instrumentation:

1. Variables that provide information needed by the operator to perform manual actions identified in the operating procedures associated with design basis accident events. These variables are restricted to preplanned actions for design basis accident events.
2. Variables needed to assess that the plant critical safety functions are accomplished or maintained, as identified in the plant safety analysis and other evaluations.
3. Variables used to monitor for the gross breach or the potential for gross breach of the fuel cladding, the reactor coolant pressure boundary or the containment.
4. Variables needed to assess the operation of individual safety-related systems.
5. Variables used in determining the magnitude of the postulated releases and continually assessing releases of radioactive materials.
6. Variables that provide information to manually actuate and to monitor the performance of non-safety-related systems to prevent unnecessary actuation of safety-related systems following plant events.

The six classifications of variables are not mutually exclusive. When a variable is included in one or more of the six classifications, the equipment monitoring this variable meets the requirements of the highest category identified.

Three categories of design and qualification criteria are used. This classification is made to identify the importance of the information and to specify the requirements placed on the accident monitoring instrumentation. Category 1 instrumentation has the highest performance requirements and is used for information that cannot be lost under any circumstances. Category 2 and Category 3 instruments are of lesser importance in determining the state of the plant and do not require the same level of operational assurance.

2.15. Mitigation and control of severe accidents

Prevention and mitigation of accidents, including severe accidents, has been an integral part of the design process for the AP600. A significant objective in the AP600 design is preventing accidents from progressing to core damage. Additional features to protect the plant fission boundaries in the event of a core damage accident have been included in the design.

The AP600 includes features specifically designed to contain anticipated core damage. The containment hydrogen control system includes hydrogen recombiners and igniters to limit the hydrogen concentration in containment so that the containment pressure boundary integrity is not challenged. Operation of the hydrogen recombiners is not required until the hydrogen concentration reaches 3.5 volume percent, which takes six days after the design basis LOCA. Igniters are available for more severe core damage scenarios with higher hydrogen generation rates. Their availability is maintained through simple post-72 hour support actions.

Another feature provided to contain core damage is the region of space located below the reactor vessel. In the extremely unlikely scenario of the core melting down and out from the reactor vessel, the space below the reactor vessel is designed to provide adequate debris bed coolability. Furthermore, the in-containment refuelling water storage tank is equipped with dump valves to guarantee release of its contents onto the containment floor for cooling the melted core.

Finally, the passive containment cooling system air-only cooling is capable of mitigating core melt scenarios for an unlimited amount of time.

3. EXTENDED LIST OF CHARACTERISTIC DATA FOR AP600

Output per reactor unit

Gross Thermal Power (MW-th)	1940 MWt
Net Electrical Output (MW-e)	600 MWe

Core and reactivity control

Fuel material	UO_2
Fuel inventory(t)	66.9 tU
Average core power density (kW/l)	78.82 kW/liter
Average fuel power density (kW/kgU)	28.89 kW/kgU
Average discharge burnup (MWd/t)	40,000 MWd/t (Nominal)
Initial enrichment or enrichment range (Wt%)	2.0 - 3.0%
Reload enrichment at the equilibrium (Wt%)	3.55% (18 month cycle)
Refueling frequency (months)	18 or 24 months
Type of refueling (on/off power)	Off power
Part of core withdrawn (%)	33%
Moderator material	Water
Active core height (m)	3.658 m
Core diameter (m)	3.361 m
Number of fuel assemblies	145
Number of fuel rods per assembly	264
Clad material	Zircaloy
Clad thickness (mm)	0.57 mm
Number of control rod/assembly	24
Type	Rod Cluster Control
Additional shutdown mechanisms	Boration
Control rod neutron absorber material	Ag-In-Cd
Soluble chemical neutron absorber	Boric acid
Burnable poison	WABA - Wet annular burnable absorber IFBA - Integral fuel burnable absorber

Reactor coolant system

Coolant medium	Borated water
Design coolant mass flow through core (kg/s)	9.19×10^3 kg/s
Cooling mode	Forced circulation
Operating coolant pressure (bar)	155 bar (15.5 MPa)
Inlet core temperature (C)	276.1°C
Outlet core temperature (C)	312.4°C

Reactor pressure vessel/tube

Overall length of assembled vessel (m)	11.59 m
Inside shell diameter (m)	3.988 m
Average shell/tube thickness (m)	0.203 m

Vessel/tube material	Carbon Steel
Lining material	Stainless Steel

Steam generator

Number of steam generators	2
Type	Delta 75
Configuration (horizontal/vertical)	Vertical
Tube material	Inconel 690-TT
Shell material	Carbon Steel
Heat transfer surface per steam generator (m-2)	6,986 m^2
Thermal capacity per steam generator (MW)	970 MWt

Pressurizer

Pressurizer total volume (m-3)	36.82 m^3
Steam volume (Full power/zero power m-3)	14.16 m^3

Main coolant pumps

Number of cooling or recirculation pumps or gas circulation	4
Type	Canned Motor
Pump mass flow rate (kg/s)	4.97 x 10^3 kg/s
Pump design rated head	73 m (240 ft.)
Pump nominal power (kW)	2240 kW

Containment

Type	Free Standing Steel
Dimension (diameter, height) (m)	39.6 m, 57.6 m
Design pressure (kg/cm^2)	3.16 kg/cm^2
Design temperature (C)	137.8°C
Design leakage rate (% per day)	0.12% per day

Safety systems or safety related systems chemical volume control system (CVCS)

Number of extraction lines	1
Number of pumps	2
Number of injection points	1
Feed and bleed connections	--

Boric Acid System

Volume of boron tank (m^3)	235 m^3 (62,000 gal)
Boron concentration (ppm)	4375 ppm
Number of injection lines	1

Emergency core cooling systems (ECCS)

H.P. Injection

Number of pumps	0 - gravity driven
Number of injection points	2

L.P. Injection

Number of pumps	0 - gravity driven injection & recirculation
Number of injection points	2

Accumulators

Number of accumulators	2
Number of injection points	2

Automatic Depressurization System

Number of lines	4 stages/8 lines total
RCS Connections	4/2 to the pressurizer 1 per each hot leg

Component cooling system (up to the ultimate heat sink)

Number of trains	2
Number of pumps	2

Emergency feedwater system	None Required

Safety related I&C system

Application of analog or digital reactor protection system	digital
Centralized safety shutdown panel	yes

Emergency power supply system

Type (diesel, gas, grid connection)	1E batteries non 1E batteries non 1E diesel/generators

AC/DC supply system

Type (rectifier, converter, battery)	Class 1E Uninterruptible Power Supply (Battery)
Estimated time reserve (hr.)	Class 1E - 72 Hrs. Non-Class 1E - 2 Hrs. (Battery)

Next page(s) left blank

BASIC INFORMATION ON DESIGN FEATURES OF THE V-407 ADVANCED REACTOR PLANT

V. FEDOROV, M. ROGOV, G. BIRYUKOV,
V. YERSHOV, B. VOLKOV
Gidropress EDO,
Podolsk

V. NOVIKOV, V. IGNATYEV
Kurchatov RSC,
Moscow

Russian Federation

Abstract

The paper describes the V-407 (or VVER-640, earlier VVER-500/600) advanced reactor plant. The paper consists of three parts: - a brief description of the plant concept; - a description of how the plant compares with the safety principles of INSAG-3 for 15 selected design areas; and - an extended data list. The concept description outlines the main elements of the safety philosophy, describes the main features of the reactor plant and its safety systems, and provides a list of main operational occurrences and design accidents, as well as beyond-design accidents. The second part discusses plant performance in the areas of: - plant process control systems; - automatic safety systems; - protection against power transient accidents; - reactor core integrity; - automatic shutdown systems; - normal heat removal; - emergency heat removal; - reactor coolant system integrity; - confinement of radioactive material; - protection of confinement structure; - monitoring of plant safety status; - preservation of control capability; - station blackout; - control of accidents within the design basis; and - mitigation and control of severe accidents. The third part, finally, presents data related to the power plant as a whole, data on reactor core and fuel, on the reactor coolant system, the reactor pressure vessel, coolant pumps, steam generators and pressurizer, and on the containment.

1. BRIEF DESCRIPTION OF THE CONCEPT

1.1. The main elements of the safety philosophy

Ensuring the safety of the personnel, the population and the environment against radiation effects is used as the basis for the design. The prescribed doses of exposure, and the standards for the release of radioactive substances and their content in the environment, should not be exceeded under normal operation, anticipated operational occurrences, and in design and beyond-design-basis accidents during the plant 50-60 years' service life.

Operating limits for fuel cladding damage are as follows:

- up to 0.1% of fuel rods with flaws of gas leaktightness, and up to 0.01% of fuel rods with direct contact between fuel and coolant,
- 7.4E10 Bcq/m^3 primary coolant iodine nuclide radioactivity,
- individual SG secondary water iodine nuclide radioactivity should not exceed 1.5E4 Bcq/m^3 under normal conditions and operational occurrences. The estimated probability of the operating limits being exceeded is less than 1E-2 per reactor-year.

Fuel element damage leading to:

- a considerable amount of radioactivity release from fuel rods,
- a considerable steam-zirconium reaction progression (considerable from the standpoint of fulfillment of the safety insurance requirements mentioned above),
- a fuel material escape out of the cladding preventing core cooling and post-accident removal,

as design limits, should not be exceeded in the design accidents. The estimated probability of the design limits being exceeded must be less than 1E-5 per reactor-year. The estimated probability of considerable fuel damage leading to the necessity of an evacuation of the population from the area prescribed by the according guides is specified to be less than 1E-7 per reactor-year.

The safety of the NPP will be achieved by consistent implementation of the "defence-in-depth" principle based on the application of a system of barriers on the path of spreading ionizing radiation and radioactive substances into the environment, as well as of a system of engineered safeguards and of organizational provisions for the protection of these barriers. The consistent implementation of the "defence-in-depth" principle means:

- installation of successive physical barriers on the path of spreading the radioactive substances: fuel matrix, fuel element cladding, primary circuit boundary, containment,
- taking into account all postulated initial events that can lead to a loss of efficiency of these barriers,
- determination, for each postulated event, of design measures and actions of operating personnel required to keep the integrity of the barriers mentioned, and to mitigate the consequences of a damage of such barriers,
- minimization of the probability of accidents resulting in an escape of radioactive substances,
- redundancy and diversity of safety systems, and physical separation of safety system trains.

The NPP considered is of the evolutionary type. The principal technical decisions have been supported by operational experience for more than 300 reactor-years of NPP with VVER-440, including the Loviisa and Paks NPPs which are known to be in the number of the best in the world measured by their load factors. More than 90 reactor-years of NPP with VVER-1000 also contribute to that base of experience.

The new design features are envisaged to be verified experimentally at a large-scale test facility (1:27 volume and power scale). The design is developed in accordance with the safety regulations for NPP /1, 2/ which meet modern world requirements. The design organizations are: OKB "Gidropress", Russian National Research Centre "Kurchatov Institute" and LIAEP, the known designers of NPP with VVER. IAEA QA requirements and the international standards ISO 9000 are taken into account in the design. In the plant safety concept, the world's modern trends in NPP safety improvements are considered in order to meet for as long a period as possible the current and future requirements for NPP safety which are constantly becoming more strict. The design passed the international examination at the NPP design competition in St.Petersburg.

The principal features characterizing the safety philosophy accepted in the design are as follows (absolute figures will be presented in other sections of this report):

- considerable decrease of specific fuel power (it is 1.25 times less than in the Loviisa NPP reactor and 1,5 times less than in a standard VVER-1000 reactor) due to an increased number of fuel assemblies,
- the fluence to the reactor vessel considered is one order of magnitude less over 60 years than that to the vessel of the standard VVER-1000 reactor over 40 years,
- the possibility of providing subcriticality with solid control rods at any moment of the life-time for a coolant temperature decrease down to 100 °C and assuming complete replacement of the boric acid in the primary circuit with pure condensate,
- retaining the large ratio of the primary and secondary coolant volumes to the reactor power typical for VVER-440 reactors (1.5-2 times more in comparison with the standard VVER-1000 reactor and Western PWRs, which provides softer temperature conditions for the core and the whole NPP equipment under transient and accident conditions),
- simplification of the operating and layout features for safety systems and all other systems of the plant (in comparison with a VVER-440 the number of pumps and compressors is reduced 4 times, the number of shut-off valves 3 times; there is a 2 time reduction in the number of high-and-low pressure tanks, and the number of sealed process penetrations is reduced by a factor of 4),
- application of horizontal steam generators with large water inventories and better conditions for natural circulation in the primary circuit in comparison with vertical steam generators,
- application of an emergency core cooling system based on the principle of passive operation that provides for the possibility of long-term residual heat removal after LOCA accidents taking also into account a possible station blackout,
- application of passive systems for residual heat removal from the reactor plant in case of a station blackout (transient),
- application of passive systems of residual heat removal from the containment,
- provision of a large water inventory inside the containment (about 2000 m^3) required to form the emergency heat removal pool, the water level of which rises above the hot legs after flooding,
- application of an inner, sealed steel shell, enclosed by an outer concrete protective shell, and both together constituting the containment system,
- application of diagnosis systems for equipment and systems important to safety for on-line diagnosis during operation and for periodic inspections after shutdown,
- application of an automatic control system of improved reliability, with self-diagnosis, and an expert system for giving advice to the operator,
- redundancy, diversity, physical separation of safety systems as part of defence in depth.

1.2. Description of the reactor plant

1.2.1. General characteristics

The design of the primary circuit uses a 4-loop configuration with horizontal steam generators. The design of the steam generators with stainless steel collectors is similar to that of VVER-440. The flow scheme and a drawing of the reactor building are shown in Figs. 1 and 2. Nomenclature, list and quantity of the reactor building components shown in Fig.1 are given in Table 1.

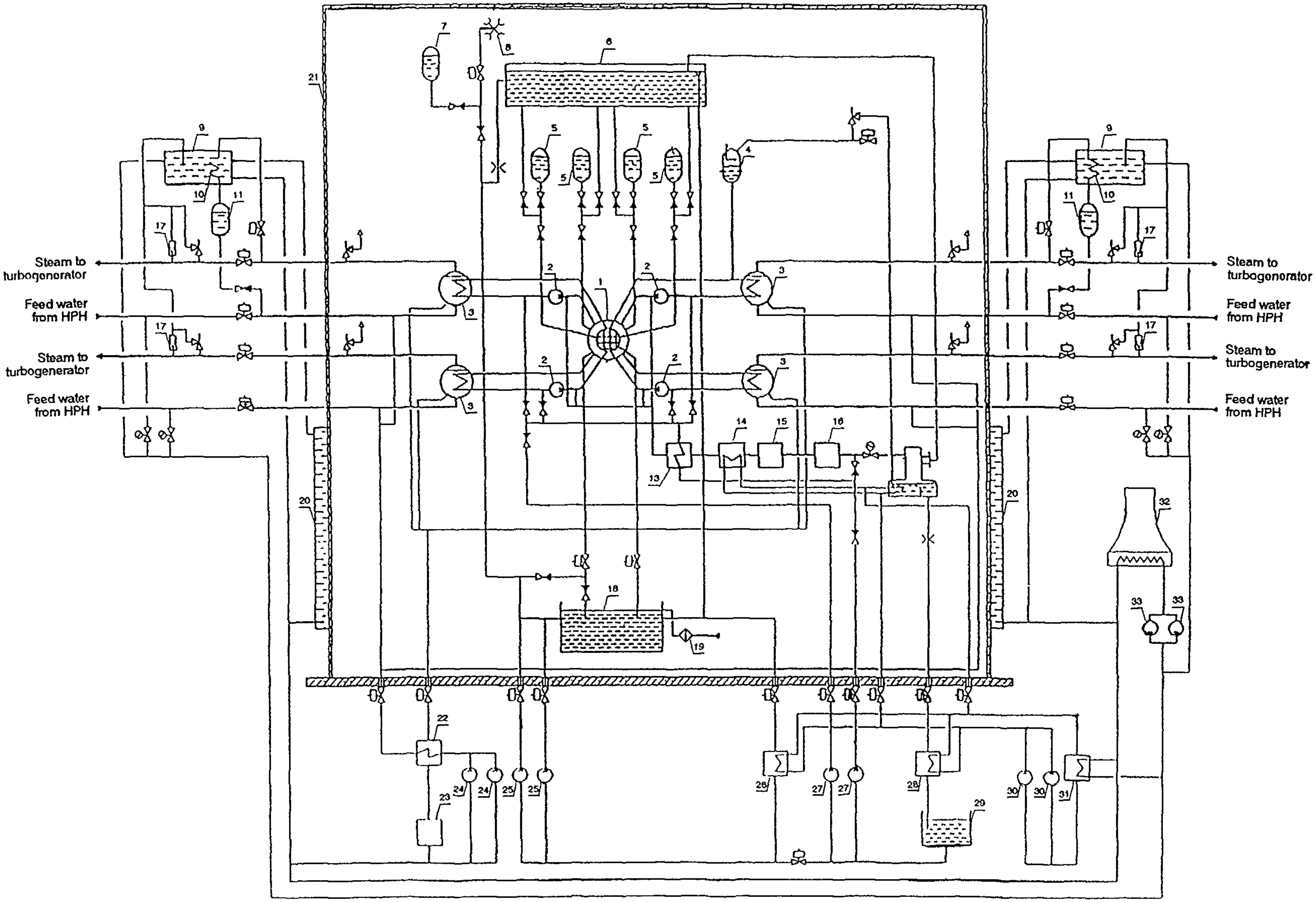


Fig. 1. Schematic diagram of reactor building system

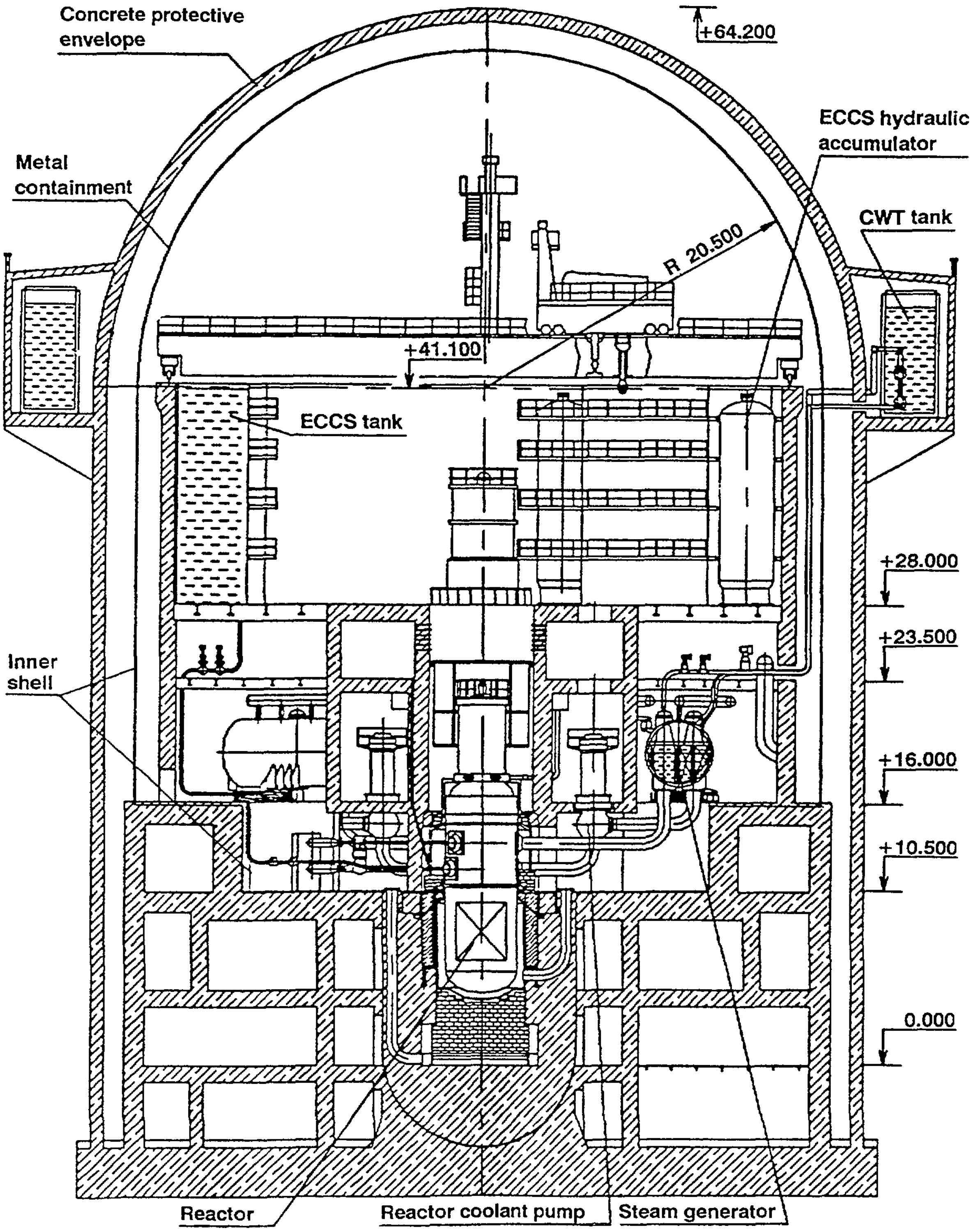


Fig. 2. Reactor building

TABLE 1: LEGEND FOR FIGURE 1

No.	Name	Quantity	No.	Name	Quantity
1	Reactor	1	18	Fuel pond	1
2	Primary coolant pump	4	19	Screen filter	2
3	Steam generator	4	20	Containment cooler	2
4	Pressurizer	1	21	Containment	1
5	HP ECCS hydrotank	4	22	Regenerative heat exchanger	2
6	ECCS atmospheric tank	4	23	Water treatment plant	1
7	Tank for Iodine fixing system	2	24	Pump of the secondary makeup-blowdown system	4
8	Sprinkler	1	25	Fuel cooling system pump	4
9	Demineralized water storage tank	4	26	Fuel cooling system heat exchanger	2
10	Heat exchanger	4	27	Primary makeup-blowdown system pump	4
11	Heat Removal System Buffer		28	Heat exchanger	1
12	Quick-acting pressure reducing device	4	29	Water tank in auxiliary system	1
13	Regenerative heat exchanger	4	30	Intermediate cooling circuit pump	4
14	Aftercooler	4	31	Intermediate cooling circuit heat exchanger	2
15	Coolant treatment plant	1	32	Dry cooling tower	1
16	Electrolyzer	2	33	Pump	4
17	Bubbler-degasser	1			

1.2.2. Reactor

Schematic drawings of the reactor are shown in Figs 3 and 4. The reactor vessel is similar to that of VVER-1000 with the exception of the nozzle zone. It is proposed to use the VVER-1000 vessel of standard production which allows to extend the service life of the V-407 reactor. The core comprises 163 fuel assemblies. A drawing of the assembly is

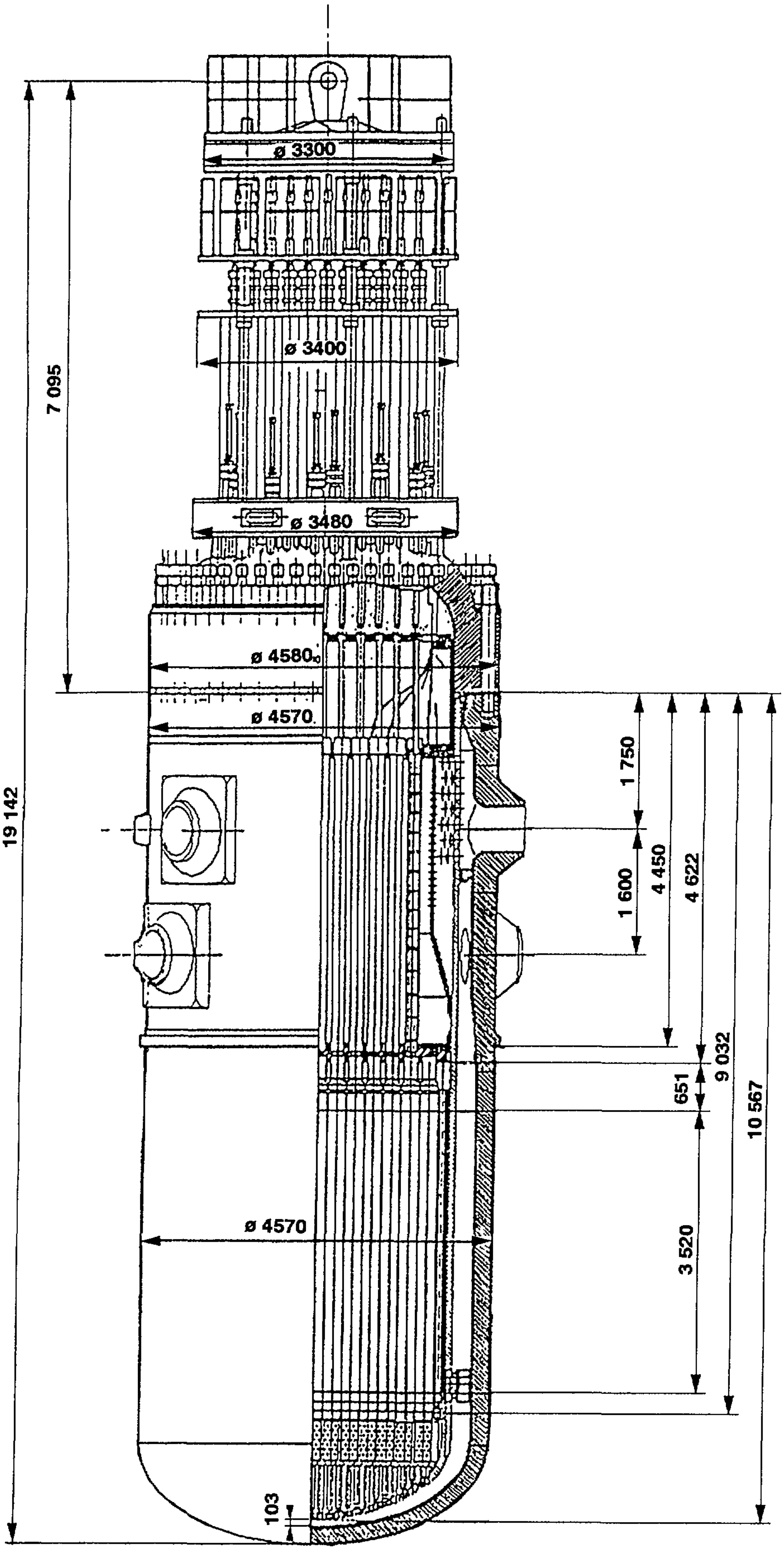


Fig. 3. Reactor

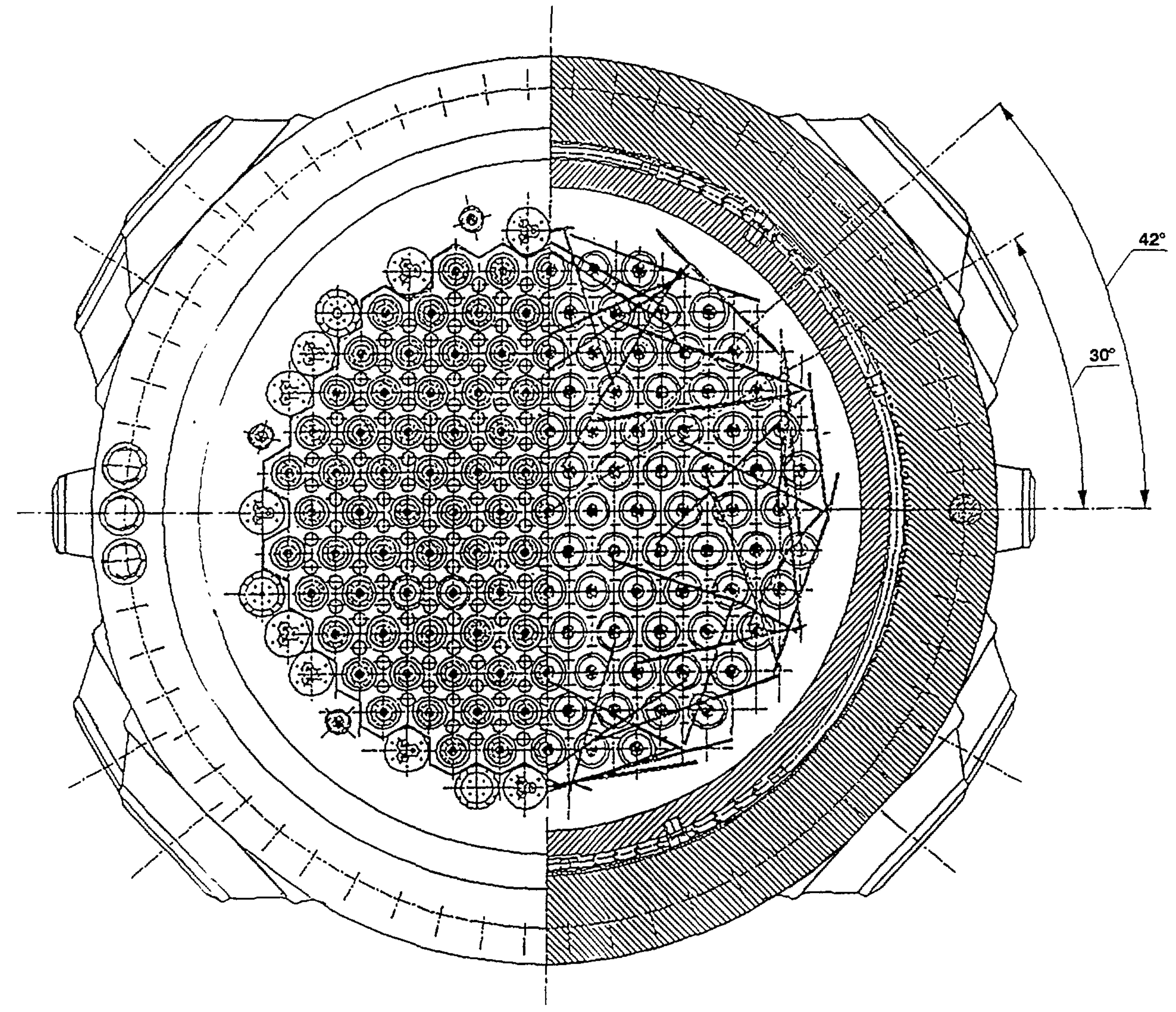


Fig. 4. Reactor

shown in Fig. 5. In the emergency protection system 121 control rods are used. A step-by-step electromagnetic (magnetic jack) drive with position indicator is used to move the control rods. The drives are installed on the reactor top head. A drawing of the control rod drive is shown in Fig. 6. Effective operation time between refuelling is 293 full power days. Average burnup of the fuel unloaded is 40 MWdays/kg. The number of fresh assemblies loaded during annual refuelling is 36.

1.2.3. Reactor coolant pump, steam generator, pressurizer

The reactor coolant pump (RCP) is of the centrifugal type in a spherical case (Fig. 7). Lubrication and cooling of the RCP are performed with water. A non-combustible lubricant is used in the electrical motor.

The steam generator is of the horizontal type (Fig. 8). For internals inspection, hatches of 500 mm diameter on both elliptic bottoms as well as hatches of 1000 mm diameter in the cylindrical part of the steam generator are provided. The pressurizer is the same as for the VVER-1000 design.

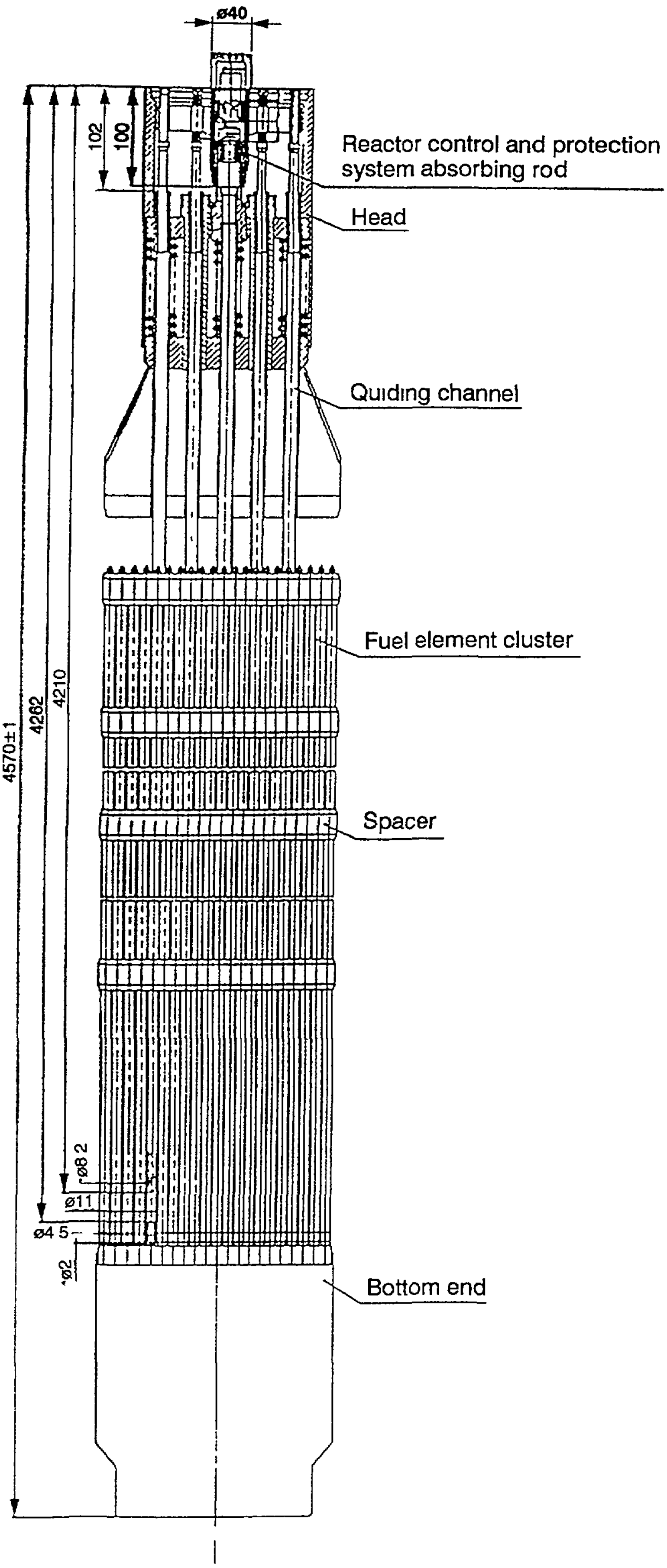


Fig. 5. Fuel assembly

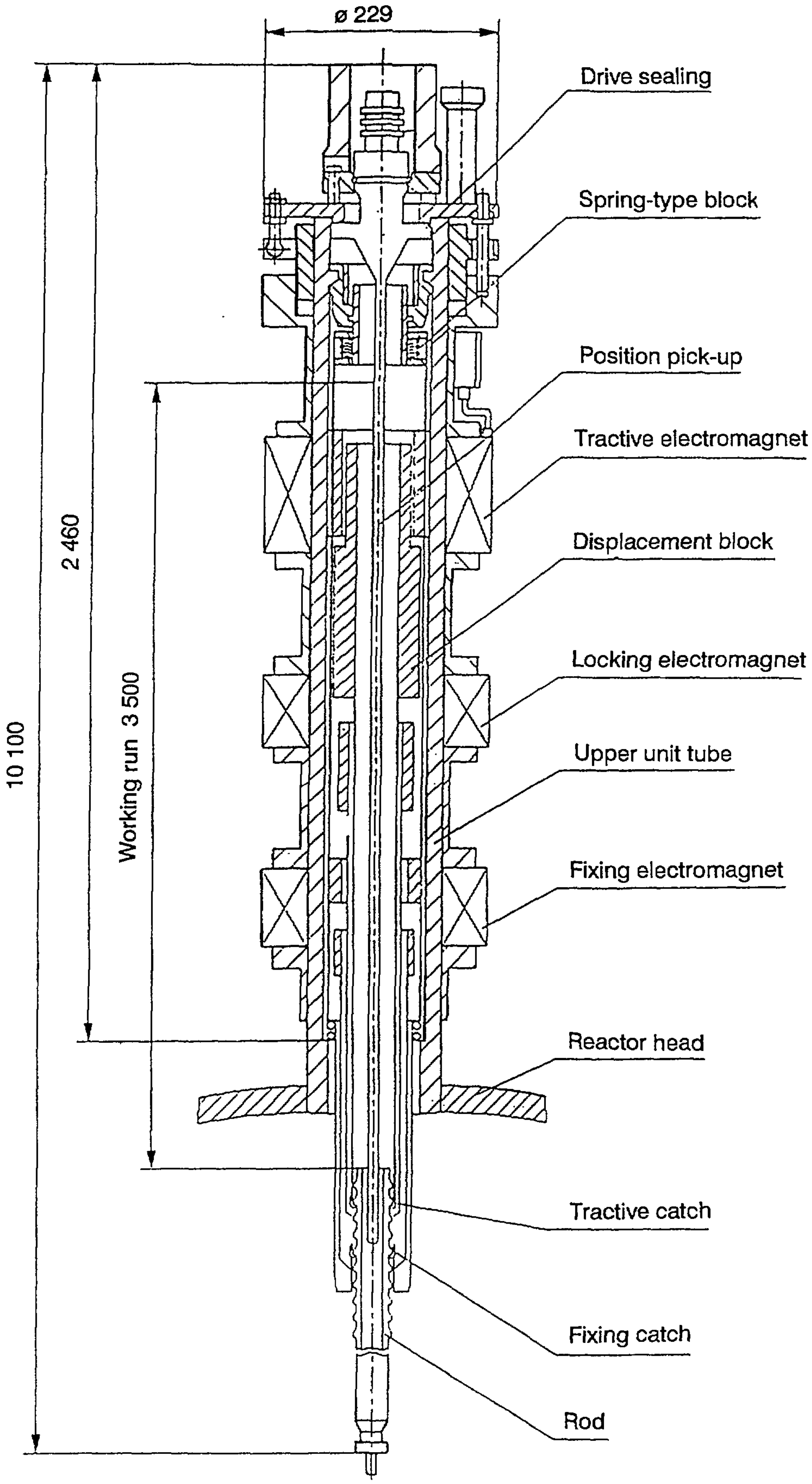


Fig. 6. Control rod drive

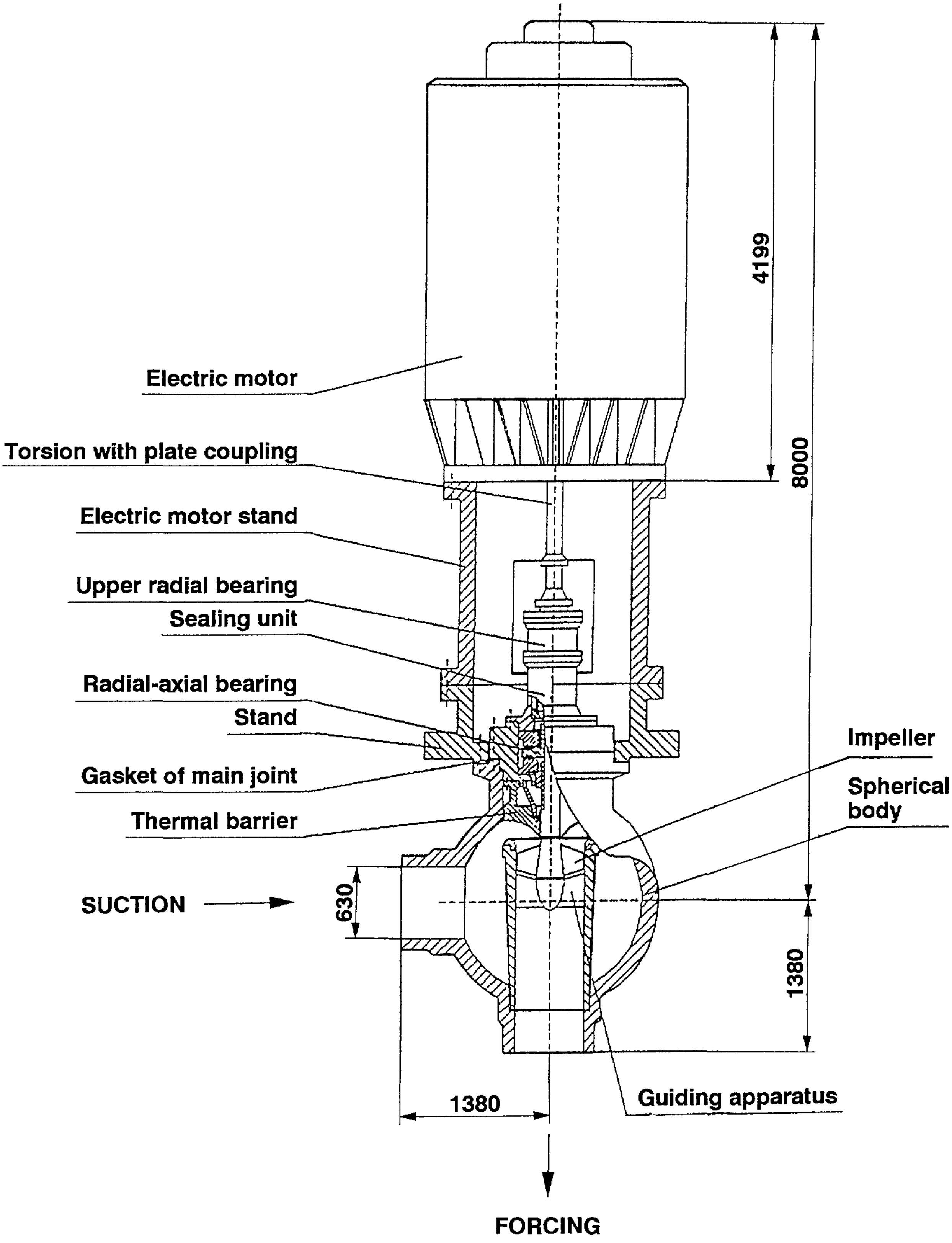


Fig. 7. Primary coolant pump

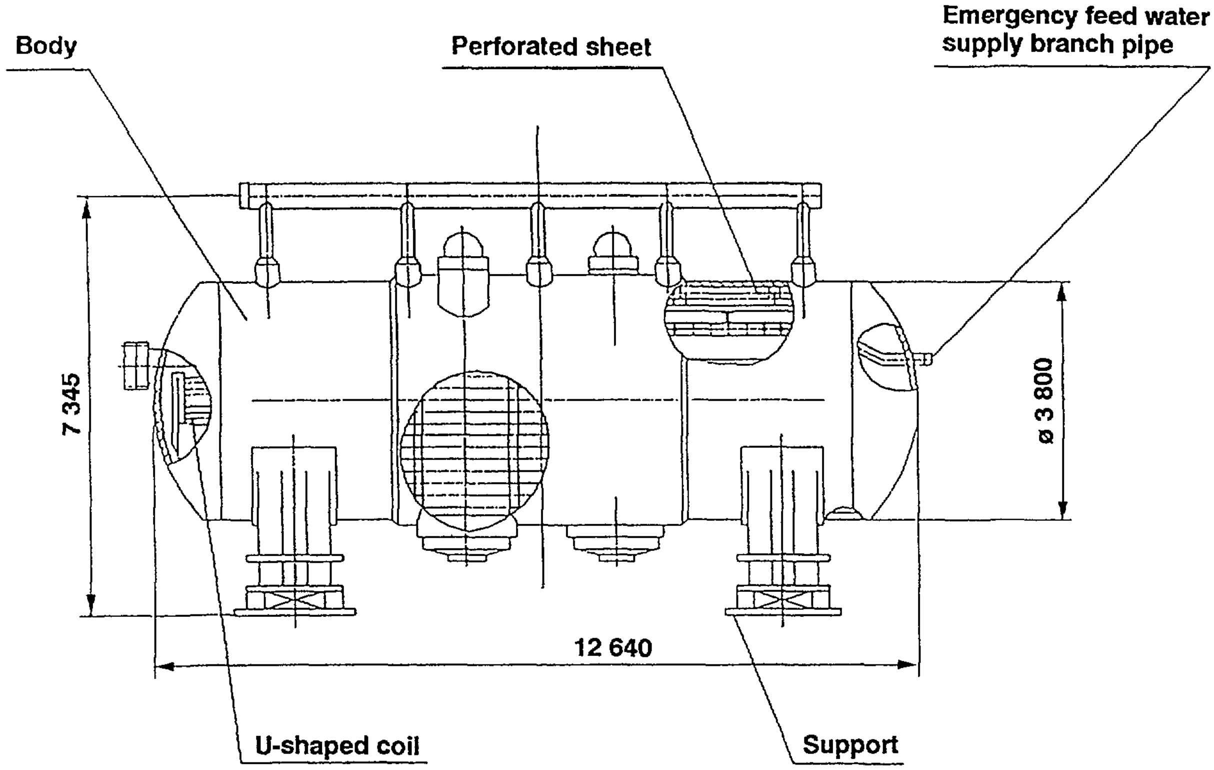


Fig. 8. Steam generator

1.2.4. Emergency core cooling system

The design employs an emergency core cooling system that is based on the principle of passive operation providing for long-term residual heat removal in LOCA accidents accompanied by a station blackout. At the first stage of the accident, the nitrogen pressurized hydrotanks will be actuated. After these are empty, the tanks holding cooling water under atmospheric pressure begin to operate. They are arranged to have a hydrostatic head of 20 m of water column in relation to the core. A pool formed around the reactor provides for residual heat removal from the core due to natural circulation.

1.2.5. System of passive residual heat removal from the reactor plant

A system of passive residual heat removal from the reactor plant is used (PHRS) in the design. The design basis of the PHRS is that in a station blackout, including loss of emergency power supply, the removal of residual heat shall be provided without damage to the reactor core, and to the primary circuit boundary, for 24 hours. Steam-water heat exchangers are used in the PHRS. These are installed in a tank of chemically demineralized water. The heat exchangers are connected to the SG secondary side such that steam from the steam generator is condensed in the heat exchanger giving its heat to the water. The condensate is returned to the steam generator. Coolant motion occurs owing to natural circulation.

1.3. List of the main design accidents (design basis accidents)

The main groups and conditions which are considered in the design in the categories of anticipated operational occurrences and accident conditions are listed below:

Reactivity-induced accidents:

- Ejection of a control rod as a result of a break of the control rod drive casing
- Uncontrolled withdrawal of a control rod bank
- Startup of an inactive reactor coolant loop at an incorrect temperature

Accidents with loss of primary coolant:

- Inadvertent opening of the pressurizer safety valve and subsequent failure to close
- Inadvertent opening of the primary circuit emergency blowdown valve and subsequent failure to close
- Small leaks with loss of coolant as a result of postulated breaks of primary pipelines with diameters less than 100 mm
- Large leaks with loss of coolant as a result of postulated breaks of primary pipelines with diameters more than 100 mm, up to the diameter of the main coolant pipe.

Accidents with loss of secondary coolant:

- Break of SG feedwater line
- Spectrum of steam line breaks inside and outside the boundaries of the containment (including the case with simultaneous break of one heat exchanger tube in the SG with the damaged steam line)
- Inadvertent opening of the steam dump valve or safety valve of a SG with subsequent failure to close

Accidents with reduction of the primary coolant flow rate

- Instantaneous seizure or break of one RCP shaft
- Loss of power to several or all RCPs
- SG primary side collector leak of equivalent hole diameter of 100 mm

Conditions with variation of turbo-generator load or feed water flow rate

- Turbo-generator load decrease
- Loss of feedwater supply
- Turbo-generator load increase

Accident situations during manipulation of fuel assemblies:

- Erroneous loading of fuel assemblies into the core and subsequent start-up
- Drop of a fuel assembly during refuelling
- Drop of loads into the reactor and into the spent fuel storage pond

Fire in NPP compartments with safety related equipment

Failure of the systems, or the equipment, related to safety assurance as a result of an earthquake or flooding.

1.4. List of beyond-design (severe) accidents

1.4.1. Design accidents accompanied by additional failures beyond single failure

1.4.2. Failure of the reactor control and protection system to operate under operational occurrences and design accidents (a wider accident spectrum than ATWS in terms of Western terminology)

Failure of the reactor and primary circuit

- Break of the core barrel
- Ejection of more than one control rod due to simultaneous failure of several control rod drive casings
- Break of the reactor vessel

Failure of the secondary circuit

- Simultaneous break of all steam lines inside or outside the containment with complete or partial failure of the shut-off valves to operate

Non-compensable leak of the spent fuel storage lining

2. DESCRIPTION OF 15 SPECIFIC DESIGN AREAS AS SELECTED FROM INSAG-3

In the following sections the reference to INSAG-3 is put in parentheses after each heading.

2.1. Plant process control systems (4.2.2.1)

Plant process control systems fulfill the automatic control of the following main controlled parameters:

- neutron flux in the core
- primary pressure
- secondary pressure
- water level in the steam generators
- water level in the pressurizer

The design value of the reactor neutron flux is maintained with the control bank of neutron absorbers, consisting of several rod cluster control assemblies, within ±2% of its nominal value.

The design value of the primary pressure is maintained by the pressurizer electric heaters and by the valves on the coolant injection line from the main coolant pump (MCP) exit side to the steam volume of the pressurizer within ±3 bar (0.3 MPa).

The design value of the secondary pressure is maintained by holding the appropriate balance of reactor power and steam flow from the steam generators to the turbine or to the steam dumping devices within ±2 bar (0.2 MPa).

The design value of the water level in the steam generators is maintained with the help of the steam generator feed water supply controller actuating the control valve on the steam generator feed water line within ±50mm of its nominal level.

The design value of the water level in the pressurizer is provided by the level controller, actuating the control valves located on the make-up line, to within ±150mm.

2.2. Automatic safety systems (4.2.2.2)

The automatic safety systems comprise:

- reactor emergency protection system
- primary overpressure protection system
- emergency core cooling system
- system of passive heat removal from the reactor plant
- system of passive heat removal from the containment
- system of quick-acting isolation valves in steamlines
- secondary overpressure protection system
- diesel-generators
- system of reliable direct current power supply

Reactor emergency protection system

The reactor emergency protection system provides a reliable switch-off of the electric power supply to the control rod drives, causing the emergency shutdown rods to drop into the core. In this case, the disappearance of the signal of the original cause does not stop the initial action of the emergency protection (see 2.5 for more detail).

Primary overpressure protection system

This system comprises two safety valves intended for the discharge of steam or a steam-water mixture from the pressurizer as its pressure increases above the permissible limit, as well as a subsystem for receiving the steam-water mixture. This subsystem involves a bubbler and pipelines connecting it with the outlets of the safety valves.

Emergency core cooling system

The emergency core cooling system (ECCS) comprises the following complex of automatically initiated subsystems:

- subsystem of hydrotanks with nitrogen under pressure
- subsystem of hydrotanks under atmospheric pressure
- subsystem of deliberate emergency depressurization

For fulfillment of ECCS functions, sources of alternating current are not required. Active elements of the system needed for the function of emergency heat removal are provided with electric power from storage batteries.

System of passive heat removal from the reactor plant

The passive heat removal system (PHRS) removes the residual reactor power during a station blackout for 24 hours. It consists of four independent trains, each of them being connected via the steam generator to the respective reactor loop. Each train has piping for steam supply and condensate return, battery operated valves, and heat exchangers for condensing the steam from the steam generator rejecting decay heat to the water tank.

System of passive heat removal from the containment

This system removes heat from the containment in accidents caused by loss-of-sealing of the primary circuit (LOCA). The main functions of the system are:

- emergency isolation of service lines passing through the containment and not pertaining to systems coping with the accident,
- removal of the heat released in the course of the accident into the containment,
- retention of radioactive products released into the containment,
- fixing of the iodine released into the containment atmosphere.

For heat removal there are provided coolers, storage tanks of cooling water and connecting pipelines in the system. Steam released to the containment condenses on the heat exchange surface of the cooler giving heat to the water of a storage tank in natural circulation. For iodine fixing, tanks with the iodine fixing solution are connected via quick-acting valves with the collector of a sprinkler device as the pressure in the containment increases. The system does not require any alternating current power supply.

Secondary overpressure protection system.

This system prevents the secondary pressure to increase above the permissible level of 115% of the secondary design pressure. It incorporates quick-acting steam dump valves and steam generator safety valves.

The system of quick-acting isolation valves in steamlines causes closing at:

- level increase in the SGs above the permissible one
- increase of radioactivity in the SGs above the permissible one
- appearance of signals indicating a steamline rupture

The system provides for:

- protection of the turbine from steam of high humidity
- prevention of radioactivity release from SGs
- restriction of steam blowing down during rupture of the secondary circuit.

Diesel generators and system of reliable D.C. power supply

Two physically separated diesel generators provide power to the safety-related systems for 2 days using its own inventory of fuel, and for an unlimited time when fuel is delivered from the outside. The system of reliable direct current power supply comprising storage batteries, provides the power supply to electromagnetic circuits for the operation of automatic safety systems as well as for recording of necessary parameters during 24 hours.

2.3. Protection against power transient accidents (4.2.3.1)

Protection against transients due to the introduction of reactivity is secured by the operation of the emergency protection (shutdown) system in response to a signal of reaching the neutron flux setting or in response to a signal of reaching the setting of reactor period decrease. Within the operating ranges the reactor's neutron power and the process parameters are maintained automatically by the reactor power controller (ARM-system). Any changes in the process variables outside the control band are made by the operators in deviation of the parameters:

- up to the set-points (PZ-2) the upward motion of the control rods is stopped;
- up to the set-points (PZ-1) type 2 preventive protection is actuated; the power reduction controller (ROM system) is switched on and a group of control rods is inserted into the core at normal speed to reach a lower power level in the reactor;
- up to emergency protection setpoints (AZ) the emergency protection system is actuated, all control rods are simultaneously inserted into the core at full speed and the reactor is tripped.

2.4. Reactor core integrity (4.2.3.2)

2.4.1. Permissible limits of fuel cladding damage

Operating limits regarding fuel cladding damage are equal to:

- 0.1% of fuel elements with the flaws of gas leaktightness type, and 0.01% of fuel elements with direct contact of nuclear fuel with coolant,
- 7.4E10 Bcq/m^3 primary coolant iodine nuclides radioactivity,
- 1.5E4 Bcq/m^3 individual SG secondary water iodine nuclides radioactivity should not be exceeded under normal conditions and operational occurrences.

There should be no fuel element damage leading to:

- considerable amount of radioactivity release from fuel elements,
- considerable extent of steam-zirconium reaction,
- fuel material escape out of the cladding impairing core cooling and to post-accident core disassembling under design accident conditions.

2.4.2. Under design conditions the following mechanical requirements are ensured:

- retention of the required geometry and position of the fuel rods in the fuel assembly, and of the fuel assemblies in the core;
- necessary margin for axial or radial expansion of fuel rods, taking into account the variation of geometry as a result of temperature and radiation effects, pressure differences and interaction between fuel pellets and fuel rod cladding;
- provision that the structure of the core is able to withstand all mechanical loads under design conditions;
- provision that the fuel rods and the fuel assemblies withstand coolant caused effects such as vibration, pressure drop, pressure pulsation and flow instabilities;
- provision of normal movement of control rods and of emergency shut down under design basis conditions.

Design features of the fuel assembly of the reactor are (see also section 3):

- triangular lattice of fuel assembly,
- value of relative thickness of fuel rod cladding such as to assure the allowable degree of interaction between fuel and fuel rod cladding during its burnup up to 50 MWd/kg, and to prevent fission product releases that would exceed the permissible level of coolant radioactivity.

2.5. Automatic shutdown systems (4.2.3.3)

The automatic shutdown system is designed for generating and executing the commands for limiting or decreasing reactor power, or for reactor shutdown when any accidents occur as a result of reactor plant failures or of operator errors. The following types of preventive and emergency commands are considered:

- sequential movement of control rod groups downwards with nominal speed up to the disappearance of the emergency signal (first type of preventive protection);
- prohibition of control rod upwards movement (second type of preventive protection);
- drop of all control rods to the lowest position (emergency shutdown);
- drop of one group of control rods downwards to the lowest position (unit accelerated preventive shutdown).

The emergency protection is actuated by de-energizing the control rod drive mechanisms. Two sets of instrumentation for generating the commands for the emergency protection are provided. The sets operate in parallel and use an "or" logic. The signals for actuating the emergency protection are generated using a "2 out of 3" logic in any set. The following physical parameters are used to generate the above mentioned protection commands:

- decrease of reactor period
- increase of neutron flux
- decrease of margin to saturation temperature in any hot leg
- increase of coolant temperature in any hot leg
- decrease of pressure differential over the reactor coolant pumps
- de-energization of several reactor coolant pumps
- decrease of pressure in the reactor
- increase of pressure in the reactor
- decrease of water level in the SG
- increase of pressure in the containment.

These parameters lead to the required decrease of reactor power, meeting the design criteria under all design conditions. Automatic disconnection of power governors and interlocking all operator's actions on control rods occur under emergency protection.

To eliminate the consequences of severe (beyond-design) accidents with the control rods assumed failed, injection of a boric acid solution with a boron concentration of 16 g/l into the hot legs is provided from ECCS tanks by two independent systems. The pumps are started up in 15 s after the voltage is applied.

2.6. Normal heat removal (4.2.3.4)

Normal heat removal is secured by coolant circulation in the primary circuit, steam generation in SGs, transfer of steam energy to the turbogenerator, and by condensation of the spent steam in the turbogenerator condenser. Scheduled cool-down is carried out at a rate of 30°C/h. Duration of the sequence is 16 hours. It proceeds in the following way:

- reactor shutdown
- increase of boron concentration to the standby value
- steam/water cool-down
- water-to-water cool-down at primary temperatures less than 130-150°C.

The same systems alongside with the emergency systems take part in heat removal from the reactor under operational occurrences and in design accidents except that the turbogenerator is disconnected after reaching the respective settings.

In the design, there are provided the necessary measures for using normal heat removal systems alongside with the ones for emergencies under beyond-design accident conditions for mitigating the consequences of these accidents and for NPP safety assurance. With this aim, the system of primary make-up is designed as two trains (2x100%) with a reliable power supply from the diesels.

2.7. Emergency heat removal (4.2.3.5)

The most typical condition for an intact primary circuit transient, specifying the highest requirements for the emergency heat removal system of the NPP, is a station blackout. In this case the heat removal from the reactor is performed by natural circulation of the coolant in the primary circuit. A system of passive residual heat removal provides emergency heat removal from the steam generators, and a cooldown of the reactor plant with a rate of up to 60°C/hour. In the case of accidents with loss of integrity of the primary circuit, the emergency heat removal is performed by the emergency core cooling system and, if necessary, by the system of passive residual heat removal.

The accumulator battery power supply is only required to put the mentioned systems into operation.

2.8. Reactor coolant system integrity (4.2.3.6)

2.8.1. General

The integrity of reactor coolant pressure boundary is provided by appropriate design and inspection during manufacturing, installation and operation. The integrity of the primary circuit is further provided by limiting the pressure of the primary coolant to below 1,1 of the operating pressure and by keeping the operating temperature below the design temperature for all design conditions. All components of the primary circuit that experience temperature stresses are subject to strength analysis and are designed with due regard for the results of this analysis. In the design, the leak-before-break concept is used.

2.8.2. Primary system overpresure protection (see also 2.2.3)

The capacity of this system assures that the allowable pressure in the primary circuit is not exceeded under all design conditions (including design accidents). The reliability of system operation is provided through compliance with the requirements of the Regulatory Norms, by selecting a supplier of high skill and competence, and by quality control at all stages of manufacture, installation and preoperational tests, and during operation.

2.8.3. Inspection and tests of the primary pressure boundaries

Inspection of the equipment state during operation provides for a timely detection of defects by:

- measurement of the parameters which deviate from their normal values to determine the soundness of the components of the system;

- check of the metal state during periodical inspections.

Preoperational, periodical in-service, and extraordinary tests of the primary pressure boundaries are performed. Extraordinary tests are performed after:

- earthquakes corresponding to the operating basis earthquake (OBE) or after one exceeding it;
- accidents which cause variation of operating parameters of equipment or pipelines beyond the design values.

Fulfillment of the necessary requirements for provision of accessibility, either for direct or remote inspection, to metal and welds is provided.

2.8.4. Determination of leaks through the primary circuit boundary in the steam generator

Check of leaks is performed by means of comparison of the primary and secondary coolant radioactivity. The check is performed using the reference isotopes J-131, J-135, Na-24, K-42 for reference. Determination of the specific radioactivity of the let-down water of each steam generator is performed once in a shift by testing the dry residue.

2.8.5. Concept of ensuring reactor vessel integrity

All materials used for the manufacture of the vessel are qualified and corroborated by long-time operational experience (90 reactor-years for VVER-1000). For the main components of the vessel and the top head ingots are produced which are then forged into rings and plates. All components of the vessel and the top head are one-piece-solid-forged. The vessel bottom and top heads as well as the nozzles in the vessel body are manufactured by die-stamp technique.

The reactor vessel is subject to inspection during manufacturing in line with the requirements of the working documents for manufacture. Geometrical dimensions and compliance with quality assurance requirements are tested both by destructive and non-destructive methods. The vessel is again inspected during the preoperational tests. In this case the reactor vessel is subject to hydraulic and non-destructive tests. Periodic examination of the reactor vessel during operation is performed with the aim of:

- detected defects control, detection and recording of metal defects;
- detection and recording of variations of physical-mechanical properties and metal structure;
- evaluation of the metal state.

All welded joints and vessel cladding are subject to non-destructive tests. Destructive tests are performed by means of testing surveillance specimens.

2.8.6. Materials of the primary pressure boundaries

The primary pipelines, the reactor coolant pump body and the steam generator tube bundles are made of austenitic stainless steel. Reactor and pressurizer vessels are made of low-alloyed carbon steel (see section 3). The rector vessel is clad with austenitic steel. Compatibility of the structural materials of the primary pressure boundary with the primary coolant is kept by the necessary water chemistry. The design fulfills the requirements for fracture toughness and brittle critical temperature of ferritic materials. Control of the variation of mechanical properties, the rate of defect growth, and the shift of brittle critical temperature of the reactor vessel metal is performed on surveillance specimens irradiated in the reactor in the areas of the highest neutron flux. Base metal cuts out of the allowance in the vessel ring opposite to the core, and of the welds are used for this surveillance.

2.9. Confinement of radioactive material (4.2.3.7)

2.9.1 Confinement of radioactive materials during normal conditions and operational occurrences is provided by maintaining the integrity of all barriers: fuel matrix, fuel rod cladding, primary pressure boundary, and containment.

2.9.2 Confinement of radioactive materials released from the primary circuit in design basis accidents is provided by maintaining containment integrity.

2.9.3 Control and confinement of radioactive materials in design basis accidents with a leak from the primary to the secondary circuit is provided by isolation of the steam generator on both the steam and water sides with the help of quick-acting shut-off valves which are actuated by a signal of radioactivity increase in the damaged steam generator.

2.9.4 Confinement of radioactive materials released from the fuel and the primary circuit in beyond-design accidents is provided by the concrete and by the bottom structures of the base of the containment, and by operation, if necessary, of the filtration plant inside the containment for the controlled removal of the atmosphere.

2.10. Protection of confinement structure (4.2.3.8)

2.10.1 Loads acting upon the outer protective shell of the containment

Seismic effects

The design is performed taking into account two levels of seismicity: an operating basis earthquake (OBE) of magnitude 7 on the MSK-64 scale and a safe shutdown earthquake (SSE) of magnitude 8 on the MSK-64 scale.

The reactor plant equipment is calculated for seismic effects proceeding from the following conditions. During operating basis earthquake normal operation of the reactor plant is to be provided. During the safe shutdown earthquake reactor and plant shutdown, cooling and fuel discharge are to be provided. All civil structures, process and electrotechnical equipment, pipelines, instrumentation, and so on, are divided into three seismic categories depending upon the degree of responsibility for safety insurance during seismic effects and on the serviceability after the earthquake. Components and systems of category 1 (the highest) shall fulfill their safety functions during and after an earthquake of SSE intensity. After an OBE serviceability is maintained.

Seismic category 1 equipment includes:

- systems for normal operation, failure of which during an SSE may result in radioactivity releases causing excessive population doses in comparison with the specified values for SSE conditions;
- safety systems for keeping the reactor in a subcritical state, for assuring emergency heat removal and for confinement of radioactive products;
- structures and equipment which could impair above functions as a consequence of an SSE.

The design considers the possibility of using special seismic isolators located under the base plate.

Loads due to wind, hurricane and tornado

The external wind load for the first category buildings and constructions is assumed to amount to 0.9 kPa, corresponding to a hurricane wind speed of 38 m/s. Effects of a tornado (sandstorm) are taken into account in the design for the first category of buildings and structures with the following characteristics and physical parameters:

- maximum horizontal speed of rotation of the tornado wall is 60 m/s;
- translational motion speed of the tornado is 15 m/s;
- tornado radius is 50 m;
- maximum wind front pressure is 3.5 kPa;
- the pressure differential between the center and the periphery of a whirlwind is 4.4 kPa;
- impact of missiles carried away by a whirlwind with a speed of 20 m/s are considered.

External industrial hazards and airplane crash:

- front pressure of the assumed explosion shock wave is 30 kPa;
- duration of the compression phase is 1s;
- direction of propagation is horizontal;
- impact of a plane with 5.7 t mass at a speed of 100 m/s is considered.

2.10.2. Loads on the inner protective steel shell:

- effect of maximum excess pressure is 0.4 MPa and the maximum temperature is 150°C taking into account design and beyond-design basis accidents;
- earthquakes as explained in paragraph 2.10.1.;
- loads during approval tests are 0.46 MPa for pressure and 20°C for temperature.

The size and the energy of missiles originating inside the containment are determined in the design with regard for the "leak before break" concept. Mechanical effects of such missiles, and of steam-water jets on the inner shell are mitigated by means of protective shields.

2.10.3. Containment protection against internal pressure

The leaktightness of the inner shell at a maximum pressure equal to 0.5MPa is not allowed to be more than 0.2% of volume per day. During design accidents the confining safety systems ensure confinement of radioactive materials inside the protective shell, heat removal from the hermetic shell, and control and suppression of hydrogen.

The following confining safety systems are provided for beyond-design accidents with severe core damage:

- system of emergency gas removal from the primary circuit;
- system of control and suppression of hydrogen (hydrogen igniters);
- system of discharge and decontamination of confinement medium (2x100%), ensuring the filtered release.

2.11. Monitoring of plant safety status (4.2.3.9)

2.11.1. Monitoring and identification of NPP safety status

The monitoring and control system provides an automated diagnosis of the state and the operating conditions of the NPP. Monitoring and presentation of information is carried out on the reactor coolant system, on the containment, on all the systems important for safety under all operating conditions of the NPP. Remote control of these systems is possible. The operating personnel monitors the NPP systems as well as the parameters defining the NPP safe status in accordance with the service manuals from the main control room (MCR). Engineered features of the on-line diagnosis system are provided to give a possibility for an operator to form a correct estimate of the plant state, and to take necessary measures during and after an accident.

2.11.2. Facilities and presentation of information important for safety

The facilities for presenting information, including displays and instrumentation for monitoring safety systems, ensure:

- indication of control rod position;
- monitoring of neutron flux during operation and refuelling;
- monitoring of the level of radioactive contamination of the ground.

The control of the following systems is ensured:

- emergency protection of reactor;
- confining system;
- safety systems;
- state of protected equipment.

2.12. Preservation of control capability (4.2.3.10)

In case of a main control room (MCR) failure, for example during a fire, the reserve control room (RCR) is used to provide:

- reactor shutdown;
- monitoring of subcriticality;
- reactor cooldown;
- putting into operation of confining systems.

The possibility of control of the systems important for safety is retained from RCR. Autonomous habitability under conditions of unavailability of regular ventilation systems is provided for the reserve control room for design events including safe shutdown earthquake (SSE) and, connected with it, fire and other site damage.

Access to the RCR is provided by an admittance check system. The RCR ensures the life support when the normal ventilation systems are de-energized in the case of anticipated impacts including SSE with accompanying fires and destructions. Local control panels which do not require interaction with the MCR and the RCR are provided. Their existence, in a number of cases, is determined by considerations of NPP layout.

2.13. Station blackout (4.2.3.11)

The normal and the emergency electric power supply system consists of two trains of 100% capacity with each channel being divided into three groups considering reliability aspects and the time interval of loss of electric power (fraction of second; time to be specified by safety conditions for various groups of equipment without increased requirements).

Start-up of the two diesel-generators, one for each channel of reliable electric power, and to be put into operation in the case of failure of the main and the reserve grid connections, is carried out in a time not exceeding 15 s from the moment of generation of a command for start up.

D.C. electric power supply of the reactor control and protection system is ensured by accumulator batteries (in each channel) designed for a discharge over 24 hours. Electric power from the accumulator batteries during a station blackout is provided for both the MCR and the RCR in full measure.

2.14. Control of accidents within the design basis (4.2.3.12)

The analysis of design accidents has been based under the condition that any intervention of operating personnel is prohibited for 10-30 min from the onset of an accident. This approach is adopted in order to exclude possible hasty and erroneous actions of the operating personnel during the first period of an accident which, as a rule, passes quickly.

It is supposed that within 10-30 min from the onset of an accident the operating personnel has had time to understand correctly the features of the accident occurred, and is able to perform the actions required in accordance with the related special manuals. Further, in case of a failure of some systems, the operating personnel has a possibility to interfere and to fulfill necessary corrective actions in accordance with the related special manuals. The provided facilities ensure the presentation of the following main information:

- accident monitoring;
- indication of control rod position;
- indication of isolating valves position;
- monitoring and check of radiation level and radioactive releases;
- monitoring and check of the reactor shutdown system and the state of safety system.

Systems ensuring automatic recording of parameters during any accidents within the design basis are provided. For a multi-unit plant each unit has a MCR from which the monitoring and control of the reactor plant and other process equipment, including safety systems, is carried out. For the purpose of decreasing the probability of errors, the operators should not take part in the control of high-speed processes. The main control room has:

- alarm light signalling of protection actuation, accompanied by powerful sound signals;
- light signalling of emergency de-energization of mechanisms, accompanied by sound of medium tone;
- warning of deviation of process parameters.

2.15. Mitigation and control of severe accidents

The operating personnel performs actions in accordance with special manuals, directed to return the plant into a controlled state during which a chain fission reaction is stopped, a continuous cooling of the fuel is established, and the confinement of radioactive products within the preset boundaries is ensured.

In the design, the work is under way to substantiate the application of engineered features which would prevent a corium release from the reactor vessel in the case of a postulated core melting.

3. EXTENDED DATA LIST

Station output

Rated thermal power of the reactor	1800 MW

Fuel assembly

Array	triangle
Number of fuel rods	294
Number of guide tubes for absorber/in core instrumentation	18/1
Full length (without control spider)	4.67 m
Fuel rod, length	3.837 m
- outside diameter	9.1 mm
- cladding material	zirconium alloy
- cladding thickness	0.61 mm
- initial internal pressure (He)	0.5 MPa
Fuel pellet, material	UO_2
- density (percentage of theoretical density)	94.5%

Reactor core

Number of fuel assemblies	163
Active height	3.53 m
Equivalent diameter	3.16 m
Rod cluster control assemblies	
- Absorber	B_4C
- Number of assemblies	121
- Absorber rods per assembly	18
Enrichments, first core	3%
reload	3.6%
$(H_20/U0_2)$ volume ratio	1.88
Average fuel burn up	40.4 MWd/kg U
Total weight of $U0_2$	68.64 t
Heat transfer surface in core	4957 m^2
Average fuel linear rating	113.4 W/cm
Peak fuel linear rating	249 W/cm
Average core voluminal rating	65.4 kW/l

Reactor Coolant System

Design conditions:	
- pressure	17.65 MPa
- temperature	350°C

Operating conditions:	
- pressure at vessel inlet	15.7 MPa
- pressure at vessel outlet	15.55 MPa
- temperature vessel inlet/outlet	293.9/323.3°C
Flow rate	53680 m^3/h

Reactor vessel

Overall height with/without the head	19.1/10.9 m
Inside diameter	4.07 m
Wall thickness (opposite to the core)	190 mm
Inlet/outlet nozzle inside diameter	620 mm
Mass (including head)	302 t
Material (forged rings)	15Kh2NMFA
Design pressure/temp.	17.65/350 MPa/°C
Neutron fluence for service life	2.5E19 n/cm^2

Reactor coolant pump

Type	centrifugal
Number	4
Design pressure/temp.	17.6/350 MPa/°C
Design flow rate	13420 m^3/h
Pump casing material	stainless steel
Speed	1500 rpm
Power at coupling, cold/hot	2600/1800 kW
Weight	72000 t
Coast down time	30 s
Pump motor inertia	1.472 t x m^2

Steam generator

Type	horizontal
Number	4
Heat transfer surface	4286 m^2
Number of heat exchanger tubes	8442
Tube dimensions	16 x 1.5
Outside/inside diameter of shell	4.1/3.8 m
Total height	7.3 m
Transport weight	300 t
Shell and tube sheet material	10GN2MFA/0Kh18N10T
Tube material	08Kh18N10T
Steam pressure at SG outlet	7.06 MPa
Steam output	894 t/h
Feed water temperature	223°C
Water Volume of secondary side	42 m^3
Steam moisture at outlet from SG	0.2%

Pressurizer

Total volume	79 m^3
Steam volume; full power/zero power	24 m^3
Design pressure/temp.	17.65/350 MPa/°C
Heating power of the heaters	2520 kW
Number of heaters	28
Outside/inside diameter	3.3/3 m
Total height	13 m
Material	10GN2MFA
Transport weight	214 t

Containment

Configuration (single or double)	double
Material	steel/reinforced concrete
Gross volume	60 000 m^3
Pressure (design)	0.5 MPa
Height/diameter	61.6/41 m
Design leak rate	0.1 % of full volume during 24 h

REFERENCES

[1] General safety regulations for nuclear power plants (OPB-88), Gosatomnadzor, USSR, Moscow, Energoatomizdat, 1990.

[2] Nuclear safety rules for reactors of nuclear power plants, PBYA RU AS-89, Moscow, 1990.

BASIC INFORMATION ON DESIGN FEATURES OF THE VPBER-600 ADVANCED REACTOR PLANT

O. SAMOILOV, V. KUUL, G. ANTONOVSKY,
A. BAKHMETYEV
Institute of Physics and Power Engineering, IPPE,
Obninsk,
Russian Federation

Abstract

The paper describes the VPBER-600 advanced reactor plant that is being developed based on the heating reactor AST-500 and experience with NSSS for ice-breakers. The paper consists of three parts: - a brief description of the plant concept; - a description of how the plant compares with the safety principles of INSAG-3 for 15 selected design areas; and - an extended data list. The concept description outlines the main elements of the safety philosophy, describes the main features of the reactor plant and its safety systems, and provides a list of design accidents and beyond-design accidents. The second part discusses plant performance in the areas of: - plant process control systems; - automatic safety systems; - protection against power transient accidents; - reactor core integrity; - automatic shutdown systems; - normal heat removal; - emergency heat removal; - reactor coolant system integrity; - confinement of radioactive material; - protection of confinement structure; - monitoring of plant safety status; - preservation of control capability; - station blackout; - control of accidents within the design basis; and - mitigation and control of severe accidents. The third part, finally, presents data related to the power plant as a whole, data on reactor core and fuel, on the reactor coolant system, the reactor pressure vessel, coolant pumps, steam generators and pressurizer, on the guard vessel, and on the containment.

1. BRIEF DESCRIPTION OF THE CONCEPT

1.1. The main elements of the safety philosophy

VPBER-600 is a medium power integral PWR placed in a guard vessel (GV). The main objective of the VPBER-600 design was to create a medium power (600 MWe) reactor plant (RP) distinguished by a qualitatively higher level of safety and by improved economic efficiency.

The problem of creating an enhanced safety RP had been solved successfully for the AST-500 heating reactor. Therefore, the principal solutions concerning the AST safety provisions, such as integral reactor layout, use of a GV and use of passive safety systems, based on diverse operation principles with deep redundancy and self-actuation, were laid into the design basis when developing the VPBER-600 power reactor with enhanced safety.

Providing the protection of the plant personnel, the population, and the environment against radiation effects is the basis for the design objective development. The prescribed doses of exposure, and the standards for the release of radioactive substances and their content in the environment, should not be exceeded under normal operation, anticipated operational occurrences, and in design basis and beyond design-basis accidents during the 60 years of the plant service life.

NPP safety will be achieved by consistent implementation of the "defence-in-depth" principle based on the application of a system of barriers on the path of spreading ionizing radiation and radioactive substances into the environment, as well as of a system of engineered safeguards and organizational provisions for the protection of these barriers. The consistent implementation of the "defence-in-depth" principle means:

- installation of successive physical barriers on the path of spreading radioactive substances: fuel matrix, fuel element cladding, primary circuit boundary, guard vessel and containment;
- taking into account all postulated initial events that can lead to a loss of efficiency of these barriers;
- determining for each postulated event design measures and actions of operating personnel, required to keep the integrity of the barriers mentioned and to mitigate the consequences of damaging such barriers;
- minimization of the probability of accidents resulting in the release of radioactive substances beyond the protective barriers;

- redundancy and diversity of systems, and physical separation of safety system trains.

A leak-tight primary system eliminating leaks during plant operation thanks to the use of canned reactor coolant pumps (RCPs), and thanks to performing boron removal by ion-exchange filters, assures a higher level of plant safety during normal operation as compared to that accomplished with traditional engineering solutions.

Reactor Plant Self-Protection is the Basis of the Design

The design relies upon the use of a reactor with intrinsic self-protection properties, passive safety systems and devices, as well as upon self-actuated devices of "direct" principle of action. This limits unfavorable consequences of failures in the external systems, loss of power, plant personnel errors and of subversive actions.

The reactor self-protection features limiting core power level, the rate of temperature rise in the reactor, and the rate of loss of coolant, are based on the following design decisions:

- reduced core power density;
- use of a core design with strong reactivity feedbacks (negative reactivity coefficients) at the expense of reduced concentration of boron in the reactor coolant, and use of burnable poison;
- elimination of large diameter primary coolant pipelines, and use of flow restrictors;
- large volume of coolant above the core;
- high level of primary coolant natural convection flow providing effective emergency residual heat removal;
- reduced neutron fluence to the reactor pressure vessel (RPV), eliminating vessel embrittlement during its operation life.

In the design, passive systems are widely used which operate on the basis of natural processes and do not need external power supplies. Such systems are as follows:

- CRDMs providing control rod insertion into the core under gravity after de-energization of the drives in response to signals of the protective system, or immediately by direct action of the working medium;

- an emergency boron injection system causing a boron solution to enter the reactor under gravity to trip the reactor;
- a passive ERHR system for cooling the reactor for at least 3 days;
- a guard vessel for keeping the core under coolant and the capability to cool the reactor down. In addition, the guard vessel acts as a reliable confinement of radioactive products after loss-of-coolant accidents;
- a containment protecting the reactor plant against external impacts, and limiting the release of radioactive products during beyond design-basis accidents.

Improvement of the reliability of the safety systems is attained by the use of self-actuated devices. They act upon the variation of working medium parameters, such as primary system pressure, pressure in the GV, or coolant level in the reactor.

1.2. Reactor plant description

A schematic diagram of the major reactor plant systems is shown in Figure 1, and the basic arrangement in the reactor building is depicted in Figures 2, 3 and 4. A legend for the name of the systems and components shown in these as well as other figures is provided in Table I.

1.2.1. Reactor

The integral reactor is characterized by arranging in a common pressure vessel the core with its control and protection systems' members, the steam generators (SGs) and the steam-gas pressurizer whose function is fulfilled by the upper plenum above the coolant surface in the reactor, as shown in Figure 5.

The integral reactor design excludes, in essence, the classes of large and medium LOCAs during primary circuit pipelines ruptures.

Normal core heat removal is effected in the forced circulation mode by six canned reactor coolant pumps. The pumps are built into the reactor bottom.

Above the core, in the annular gap between the reactor pressure vessel and the in-vessel barrel, the heat-exchange surfaces of the SGs are arranged. (cf. Figure 6.) The SG is of the once-through type, consisting of 12 independent sections.

At the core inlet there is a pressure chamber assuring uniform distribution of the coolant flow through the core fuel assemblies (FAs).

The simplicity of the circulation circuit assures a high level of natural convection flow, and the capability for a reliable cooling of the core by natural convection in all emergency situations, including the steam-condensation mode after loss-of-coolant accidents.

One of the features of the integral layout is a large water gap between the core and the reactor vessel serving as a radiation protection. Therefore, the neutron fluence is less than 10^{17}n/cm^2 which eliminates the problem of reactor vessel metal property degradation under irradiation.

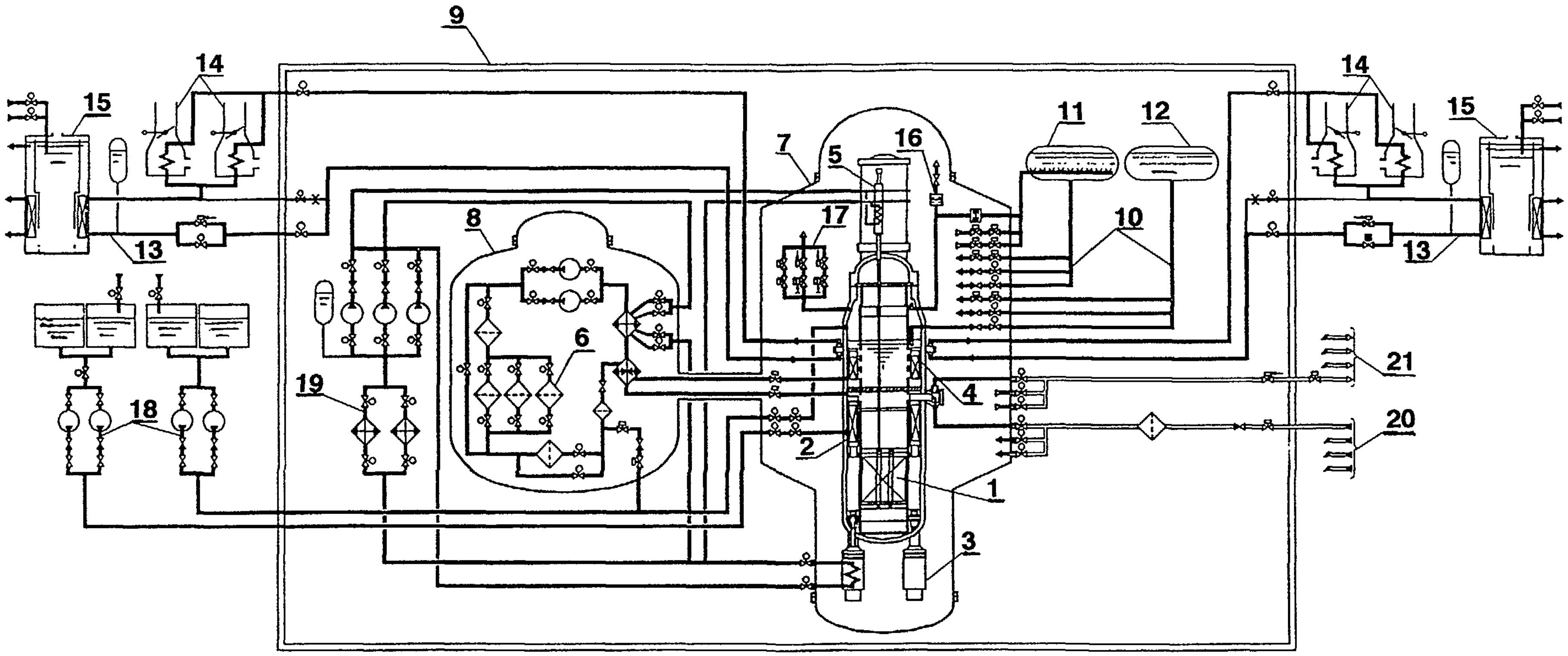


Fig. 1. Schematic diagram of reactor building system
(For explanations see TABLE I.)

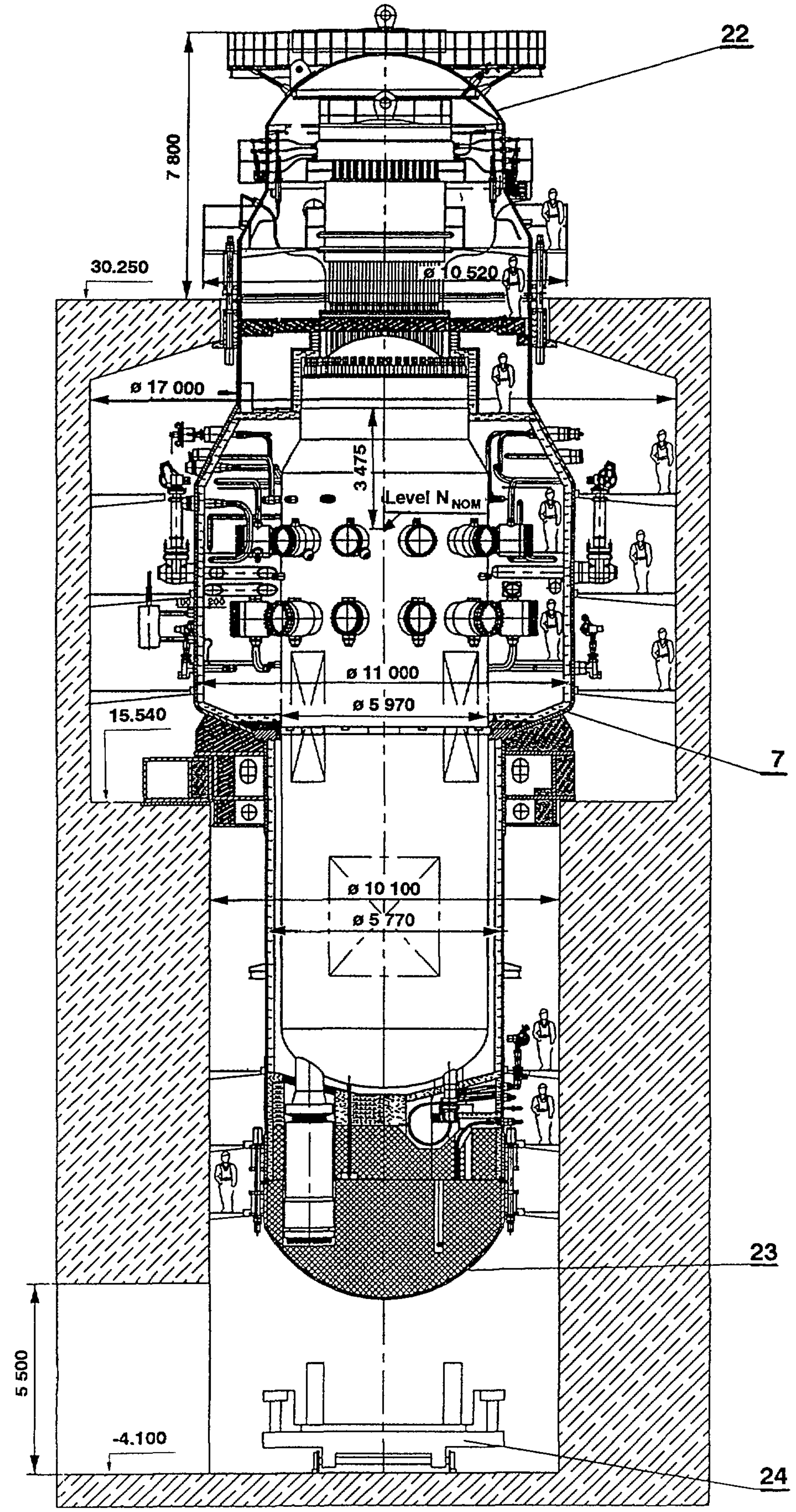


Fig. 2. Reactor in guard vessel
(For explanations see TABLE I.)

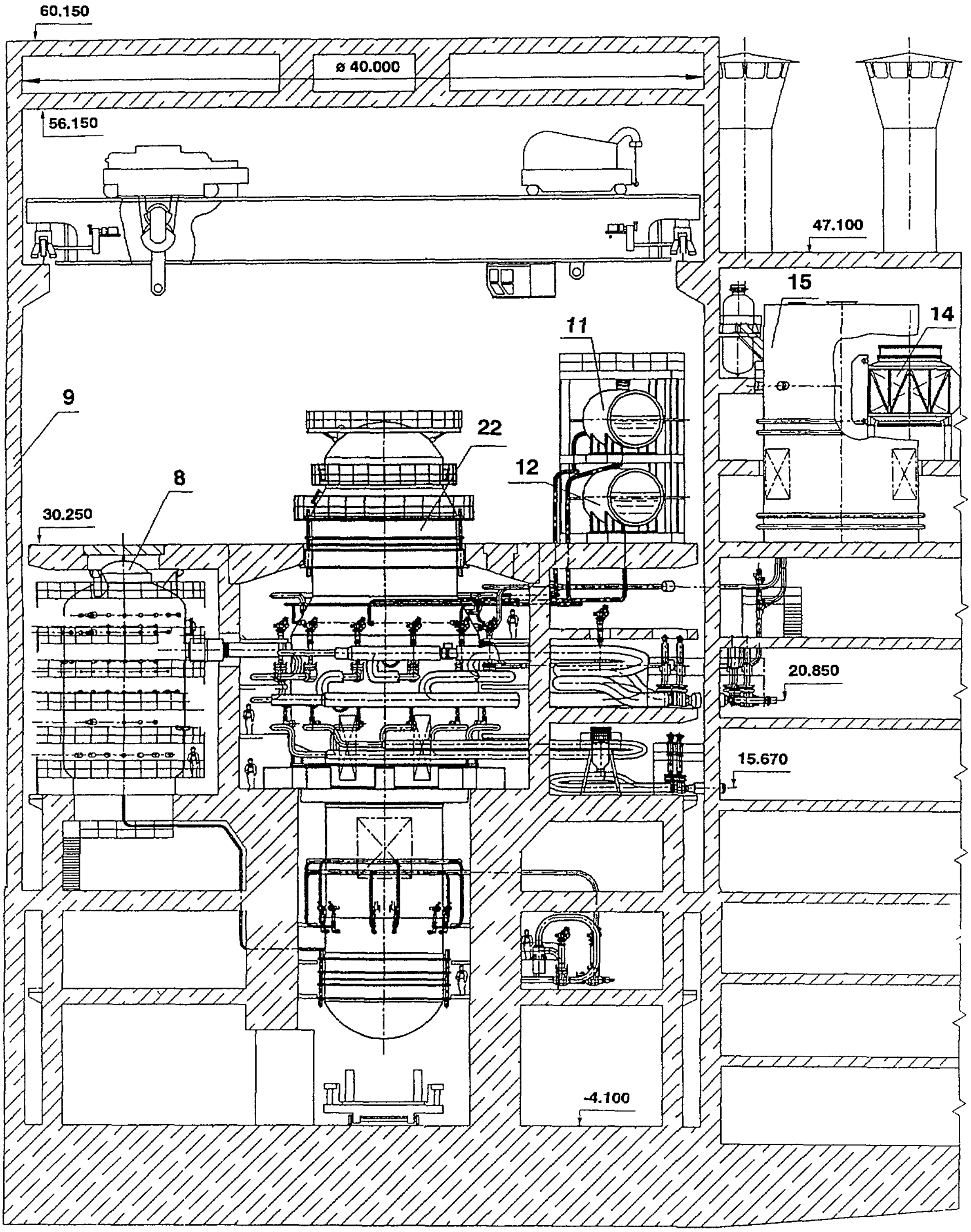


Fig. 3. Reactor building
(For explanations see TABLE I.)

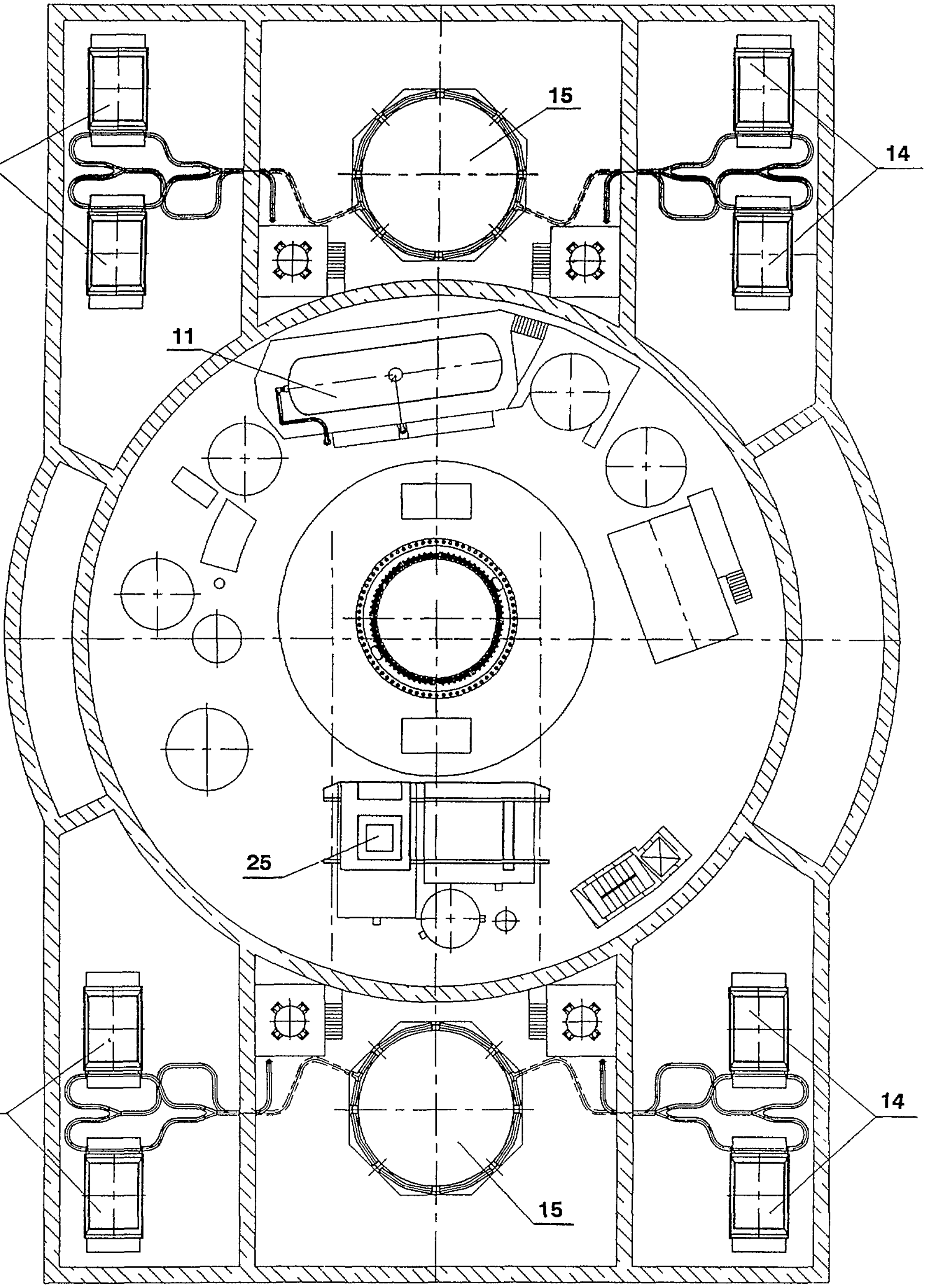


Fig. 4. Reactor building
(For explanations see TABLE I.)

TABLE I. LEGEND CORRESPONDING TO FIGURES 1 - 6

No	Name	No	Name
1	Reactor	15	Units of water heat exchangers
2	Steam generator	16	Overpressure protection system
3	Reactor coolant pump	17	Reactor de-pressurizing system
4	ERHR heat exchanger-condenser	18	Primary coolant make-up system
5	CRDM	19	Primary equipment cooling system intermediate circuit
6	Coolant purification and boron control system	20	Feed water
7	Guard vessel of reactor	21	Steam to consumers
8	Guard vessel of purification system	22	Removable part of GV
9	Containment	23	GV bottom
10	Emergency boron injection system	24	Lifting-transport machine
11	Boron solution storage tank	25	Refuelling machine
12	Boron solution filled hydroaccumulator	26	Reactor core
13	ERHR system	27	Reactor pressure vessel
14	Air heat exchangers	28	Reactor closure head

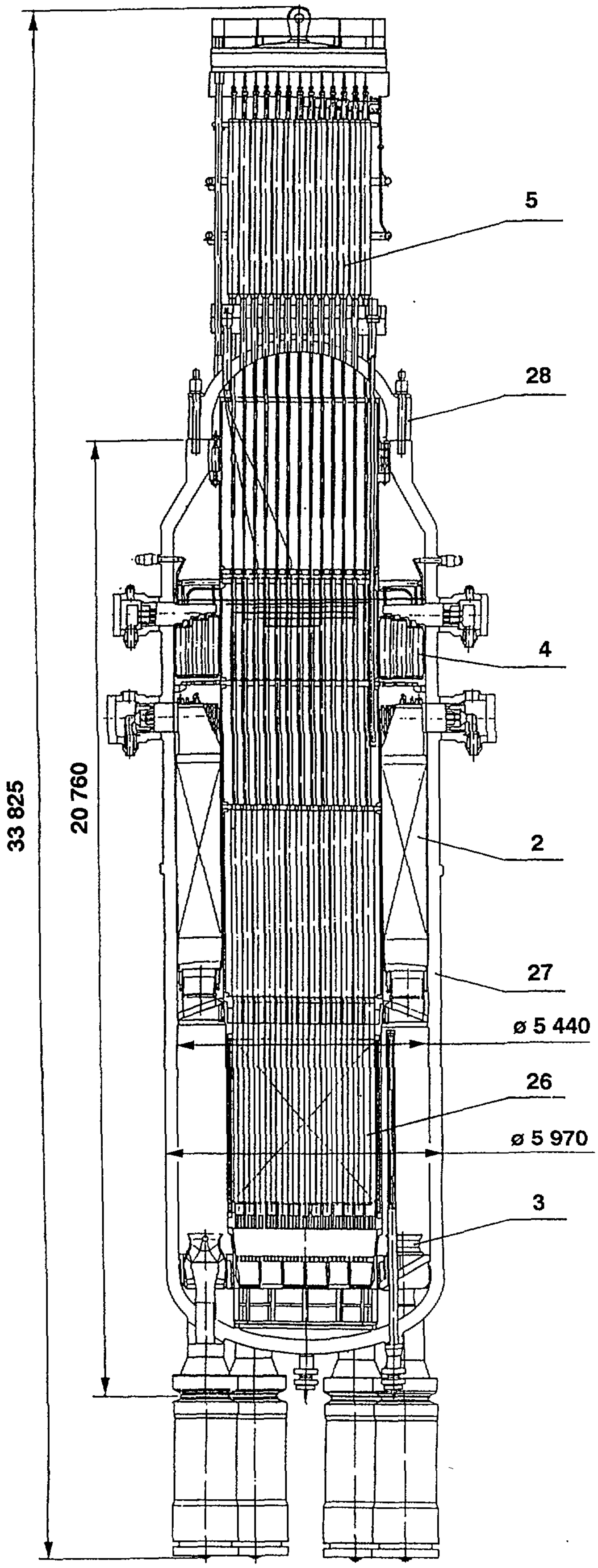


Fig. 5. Reactor
(For explanations see TABLE I.)

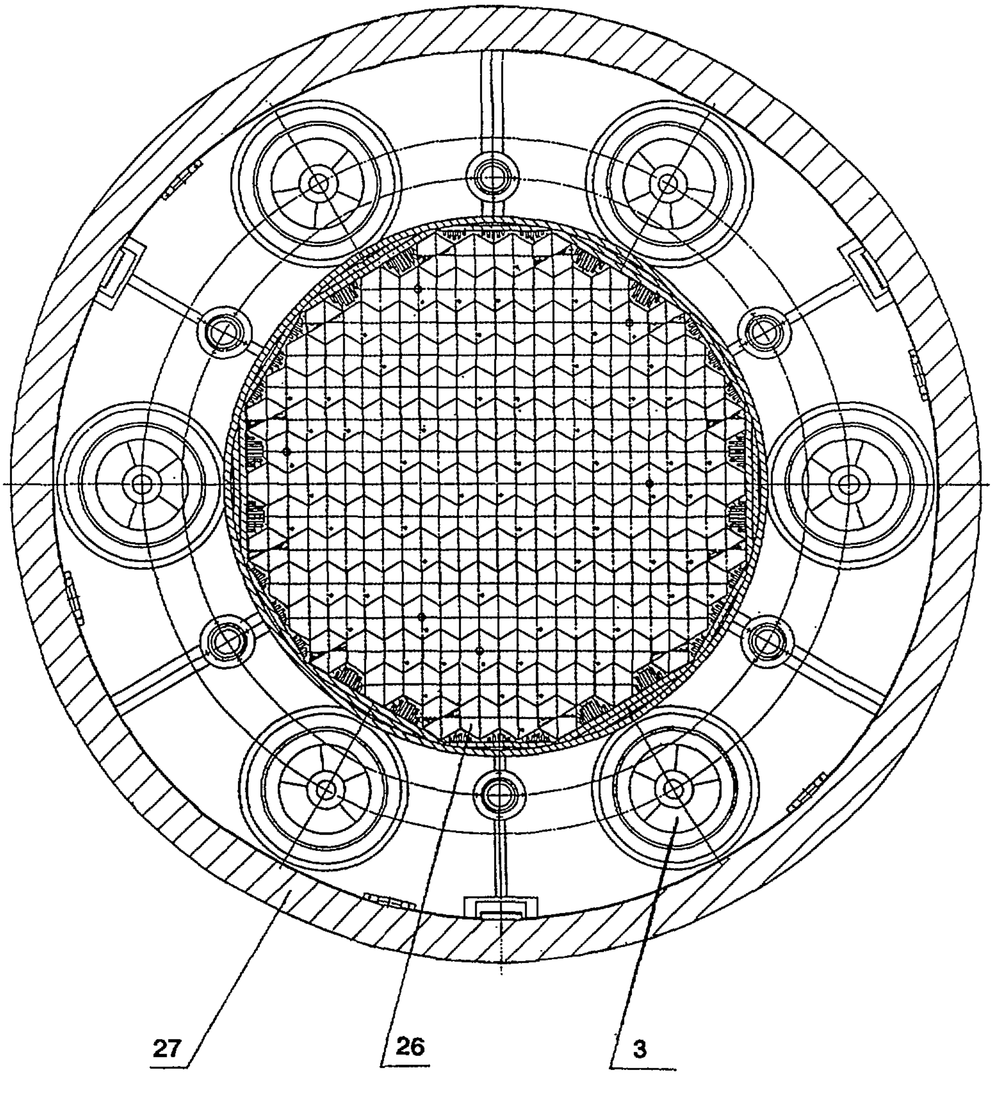


Fig. 6. Reactor
(For explanations see TABLE I.)

Above the SGs, but still under the coolant level, heat exchangers/condensers are arranged for emergency removal of reactor residual heat. They operate as condensers in case of primary circuit loss of integrity.

The electromechanical CRDMs are installed on the reactor cover. They move the working members of the control and protection system in the power regulation mode, and release them under emergency protection conditions.

In a space between the in-vessel barrel and the reactor pressure vessel the ionization chambers are suspended at core level. The core consists of hexagonal Fas. Fuel rods are used which are similar to those used in VVER reactors.

A highly effective mechanical system for reactivity compensation is used. The working members of the control and protection system (CPS) are available in the majority of the core FAs. By the mechanical system a subcritical state of a cold and clean core can be assured without boric acid addition to the moderator. Compensation of the reactivity margin for fuel burnup is provided by combined action of CPS working members, boric acid in the coolant and self-shielded burnable poison.

The core allows to realize various fuel cycles distinguished by the number of reloadings per core lifetime. Fuel average burnup is 52000 MWd/tU. The reactor refuelling interval is two years.

The reactor and all the systems which operate under primary circuit pressure are arranged in the guard vessel.

1.2.2. Safety systems

The emergency protection (EP) system is intended to terminate, or limit the chain reaction when an emergency situation arises, or when there is a deviation from normal operating conditions. The top level of protection triggers the insertion of all CPS's working members into the core with maximum speed (following drive motor de-energization).

The passive emergency boron injection system is intended for bringing the core into a subcritical state, and keeping it in this state, in case the CPS drives fail to actuate. Actuation of one of the tanks containing boron solution is effected by opening the pneumatically-driven valves in the pipelines connecting the tanks with the reactor, or by rupture of a membrane through the direct action of the pressure in the reactor. The boron solution enters into the reactor by gravity due to the elevated location of the tank above the reactor after equalization of the pressures in the reactor and in the tank. The second tank, intended for reactor shutdown in LOCA accidents, is passively actuated on the basis of the hydro-accumulator principle.

The passive heat removal systems operate in natural circulation of the coolant. The heat is removed through an intermediate circuit. The actuation of passive heat removal systems in case of an accident is provided by opening the valves draining the water from the water heat exchangers (HXs) both in response to signals from the automatic control system, and directly by the action of pressure or water level in the reactor.

During reactor cool down, residual heat is removed by the HXs-condensers of the passive and continuous heat removal systems. The heat is then transferred to water storage tanks through which service water is circulated. In case of loss of service water, heat is removed by evaporation of water from the tanks. Use of air HXs is considered which remove the residual heat after evaporation of the water from the tanks for an unlimited time. A reactor depressurization system is intended for the case of beyond design-basis accidents associated with a reactor pressure vessel loss of integrity in its lower part.

The GV is a passive protective and localizing device assuring safety after primary circuit ruptures, and after a loss of reactor vessel integrity within the limits of technically possible size. The GV is designed for the pressure building up after a primary circuit loss of integrity, and serves for keeping the core covered with coolant, assuring both the heat removal from the reactor and the confinement of radioactive products.

The system of localizing valves is intended for isolation of a SG in case the integrity of its tubing or pipelines is lost.

In each SG section there are electrically-driven localizing valves welded to the GV. In each loop double, pneumatically-driven, localizing valves are installed, one group of which actuates in response to the automatic control system signals, while the other one actuates directly to the signal indicating a drop of coolant level in the reactor. A check valve and pneumatically driven localizing valves are installed on the feedwater pipelines.

1.2.3. Reactor design validation

The development of the reactor plant design is based on the experience with the construction and successful operation of the NSSS for ice-breakers, and on the basis of the AST-500 reactor development. In this regard, despite the novelty of the design in general, the VPBER-600 can be considered as an evolutionary type reactor. The concept of the plant design is based on the use of operating-experience proven equipment with high lifetime characteristics.

The engineering solutions for the plant equipment such as canned RCPs, once through SG, GV, and passive self-actuated devices have been developed and validated comprehensively.

Canned circulation pumps with operating conditions not easier than those for the pumps for VPBER-600 have gone through comprehensive development and testing. As part of ice-breakers' NSSS, they have already been operated for more than 20 years, with more than 100 thousand hours of operation without losing their operability.

The design of once-through SGs is experimentally proven; such SGs have gone through comprehensive tests, and operate according to specified characteristics in nuclear power plants. The fabrication technology for SGs with large number of steam generating elements is mastered, and their mass production is organized.

The GV proposed is of the same design as for AST-500. It has gone through comprehensive tests during design and development, and during manufacturing. The compartments of marine nuclear power plants, corresponding in size and materials to the VPBER-600 GV, are serially produced by the home industry.

Passive self-actuated devices, such as pressure-actuated electric current breakers, hydrocontrolled pneumo-distributors, membrane safety valves, are widely used in AST-500 and in NSSS for ice-breakers; they have gone through extensive tests and are accepted for industrial production.

The main technological issues associated with reactor pressure vessel fabrication have been solved. The VPBER-600 equipment structure is such that it allows to perform extensive experimental development of individual items, assemblies, units, etc. in test facilities with verification of all specified characteristics before putting the NPP into operation.

1.3. Design accidents

1.3.1 Inadvertent change of reactivity

- Inadvertent upward movement of one control rod or of a group of control rods being moved simultaneously

- Control rod movement caused by a CRDM stand pipe breaking off
- Drop of a control rod, moving down a group of simultaneously moved control rods at working speed
- Decrease in concentration of boric acid in the coolant
- Inadvertent startup of the main primary coolant pumps
- Increase in steam flow rate
- Steam line rupture inside the guard vessel
- Steam line rupture outside the guard vessel
- Decrease in feed water temperature
- False actuation of the passive residual heat removal system
- Erroneous loading of a fuel assembly into the core.

1.3.2. Disturbance of heat removal from the reactor

- Loss of off-site power
- Termination of steam delivery to a turbine
- Feedwater loss
- Switch off (loss of power) of a portion or all main coolant pumps
- Seizure of one main coolant pump
- Inadvertent closure of steam or feedwater isolation valves on a SG.

1.3.3. Loss of coolant accidents

- Rupture of maximum diameter primary pipeline inside the guard vessel
- Steam generator tube rupture
- Rupture of SG maximum diameter piping
- Loss of tightness between the primary circuit and the intermediate circuit of the reactor equipment cooling system
- Loss of tightness between primary and ERHR circuits.

1.3.4. Disturbances during reactor refuelling

- Drop of fuel assembly into the reactor
- Drop of a container with spent fuel
- Loss of power during refuelling

1.3.5. Fire in NPP compartments with safety related equipment

1.3.6. Failure of systems, or equipment, related to safety assurance as a result of earthquake or flooding

1.4. Beyond-design accidents

1.4.1. Loss of coolant accidents

- Primary circuit piping rupture with loss of power and failure of automatic actuation of the reactor protection and the ERHR systems
- Loss of RPV integrity in the bottom part or in the nozzle of the main coolant pump of technically possible size
- Rupture of a SG tube with failure to close the isolation valves for 24 hrs
- Rupture of SG maximum diameter piping with failure to close the isolation valves for 24 hrs.

1.4.2. Emergency transients

- Station black out for 72 hr (loss of auxiliary power supply and of standby diesel generators) with failure to automatically actuate the reactor protection and ERHR systems
- Loss of heat removal from the reactor with failure to connect the passive ERHR systems channels
- Steam line rupture with failure of automatic actuation of the reactor protection system
- Transients with one of a large number of control rods stuck
- Inadvertent upward movement of a group of simultaneously moved control rods with failure to actuate the automatic protection system.

2. DESCRIPTION OF 15 SPECIFIC DESIGN AREAS AS SELECTED FROM INSAG-3

In the following sections the reference to INSAG-3 is put in parentheses after each heading.

2.1. Plant process control systems (4.2.2.1)

The plant process control system fulfills the automatic control of the following main parameters of the primary and secondary circuits:

- reactor power,
- primary pressure,
- steam pressure.

The reactor power is changed according to the requested plant output by appropriate variation of the feedwater flow rate to the steam generators. Feedwater flow control is carried out by the "feed integrated device" (throttling and control valves) within 2% of its nominal value.

The design value of the primary pressure is maintained by moving of individual control banks comprising several absorber rod clusters. The accuracy maintaining the primary pressure is 0.15 MPa.

The design value of the live steam pressure is maintained by the turbine control valve with an accuracy of 0.1 MPa.

2.2. Automatic safety systems (4.2.2.2)

2.2.1. List of automatic safety systems:

- reactor emergency protection system;
- passive boron injection system;
- emergency residual heat removal system;

- reactor depressurizing system;
- primary overpressure protection system;
- quick-acting isolation valve system for steam and feedwater lines;
- diesel generators, reliable DC power supply system.

2.2.2. Reactor emergency protection system

The reactor emergency protection system provides reliable de-energizing of the CRDMs in response to the emergency protection signals (see specific area 2.5). In case the signal disappears, the starting protective action is not interrupted.

De-energizing the CRDMs to scram the reactor is effected with the help of self-actuated devices directly actuated by the primary pressure if the pressure exceeds the emergency protection setting for the primary pressure. The reactor is also scrammed by direct action of the pressure in the guard vessel.

2.2.3. Passive boron injection system

The emergency passive boron injection system is intended to reduce the reactivity of the core and to maintain it in a subcritical state in case the CRDMs fail to actuate. The system comprises two storage tanks containing concentrated boron solution. Putting one of the tanks into action is provided by opening the pneumatically-driven valves in the pipelines connecting the tank with the reactor, or by rupture of a membrane under the force of the primary pressure. After equalizing the pressures both in the reactor and in the tank, the boron solution enters the reactor under gravity due to the tank elevation above the reactor.

The pressure setting for actuating the membrane exceeds the one for actuation of the CRDMs. The second tank is a hydro-accumulator which is activated passively in loss-of-primary-circuit-integrity accidents.

2.2.4. Emergency residual heat removal system

The passive emergency residual heat removal system operates in natural convection of the coolant, transferring the core decay heat to the cooling water, or by evaporation of the water in the storage tanks of the heat exchanger units. The core decay heat is removed via the intermediate circuit which has a higher pressure compared to that in the reactor.

The water inventory is sufficient for continuous operation of the system for 3 days under loss-of-power conditions. Following the evaporation of the water, the core decay heat is dissipated through air heat exchangers. The system is composed of four independent trains of 50% capacity each. The water heat exchangers are arranged by pairs in the two tanks.

The system is started in the event of an accident by opening the valves in the pipelines for draining water from the heat exchangers in response to signals of the automatic control system or directly by reactor pressure or reactor coolant level. Diverse valves are used in the trains of the system.

2.2.5. Reactor depressurization system

The reactor depressurization system prevents ejecting water from the reactor by the pressure in the steam-gas pressurizer in the event of beyond design accidents caused by loss of integrity in the bottom part of the reactor vessel or in the RCP nozzle or casing.

At a pressure increase in the guard vessel, and after a significant lowering of the coolant level in the reactor, the pressure relief valves of the pressurizer open. A steam-water mixture is dumped into the guard vessel, causing a pressure equalization between reactor and guard vessel which terminates the coolant outflow. The system is actuated in response to signals of the automatic control system, or immediately by the pressure in the guard vessel, or by the coolant level in the reactor.

The system consists of two independent trains. There is a third independent train for remote actuation.

2.2.6. Primary overpressure protection system

The system is intended to protect the reactor against an inadmissible rise of pressure in beyond-design accidents. The system setting exceeds those for the reactor automatic emergency protection system, for the emergency protection by direct action of pressure in the reactor, and for the emergency boron injection system membrane rupture.

The system uses a safeguard integrated device (membrane plus valve) providing for steam-gas mixture dumping from the pressurizer into the guard vessel.

2.2.7. Quick-acting isolation valve system for steam and feedwater lines

Each of the four secondary loops is provided with a quick-acting isolation valve which closes when the coolant level in the reactor drops, and so disconnects a loop with a leaky section of the SG. The valve closes both to signals from the reactor automatic control system, and immediately to the action of the coolant level in the reactor.

In addition, there are remotely-controlled valves to isolate leaky sections of the SG. They operate in response to signals from the steam radioactivity monitoring system.

2.2.8. Diesel generators, reliable DC power supply system

The two separated diesel generators have stored sufficient fuel for providing power to the safety systems for several days. They are switched on remotely because the passive means provide a long grace period (hours and even days).

2.3. Protection against power transient accidents (4.2.3.1)

The reactor core has been developed proceeding from the requirement to ensure negative reactivity feedbacks (void and temperature reactivity coefficients) over the entire range of the reactor parameter variation.

The electromechanical control system reactivity worth, the control rod travelling velocity and their grouping, are selected in such a way that a technically possible rate of positive reactivity addition is limited and virtually insignificant. The number of control rods that can be moved simultaneously is limited by appropriately engineered means. A control rod ejection after rupture of its casing is excluded. In the event of CRDMs de-energization reactor scram is provided with maximum speed.

Reactor protection in reactivity accidents is provided by the emergency protection system actuation in response to the signal of reaching the settings for neutron power or reactor period.

Several levels for the reactor protection are provided:

- 2nd type preventive protection: withdrawal of the control rods prohibited;
- 1st type preventive protection: one or several control rod banks are inserted into the core with maximum velocity to reduce the reactor power;
- emergency protection: all control rods are inserted into the core simultaneously with maximum velocity, resulting in reactor trip.

The ionization chambers are arranged in the RPV and provide neutron flux and period monitoring over the entire range of neutron flux density variation during the reactor operation.

2.4. Reactor core integrity (4.2.3.2)

2.4.1. Permissible limits for fuel cladding damage

The following operating limits regarding fuel cladding damage are adopted:

- fraction of gas-leaky fuel rods equals to 0.2% and to 0.02% for fuel rods having direct contact of nuclear fuel with reactor coolant;
- $2.0\text{x}10^{10}$ Bq/m^3 reactor coolant iodine nuclide radioactivity;
- $1.5\text{x}10^{3}$ Bq/m^3 secondary coolant radioactivity for individual nuclide should not be exceeded under normal and abnormal conditions.

2.4.2. Under design conditions the following is ensured:

- preservation of the fuel rods and their position in a fuel assembly, as well as of the fuel assembly in the core;
- needed margin for axial and radial expansion of fuel rods, taking into account their geometry variation resulting from thermal and radiation effects, pressure differences and fuel pellet-cladding interaction; core capable to withstand all design mechanical loads;
- stability of fuel rods and fuel assemblies under coolant flow-induced effects such as vibration, pressure drop and pulsation, flow instabilities;
- normal movement of control rods and reactor trip under design basis conditions.

The integral design of the reactor unit allows to exclude large-diameter primary pipelines and thus the accidents associated with such pipeline ruptures. This approach precludes the appearance of strong dynamic impacts affecting the core structural items.

Design features of the fuel assembly (see also section 3).

- triangular lattice fuel rod arrangement;

- relatively thick cladding to assure the allowable level of fuel effect upon the cladding at a burnup of 52 MWd/kg and to prevent exceeding the permissible level of the reactor coolant radioactivity.

Reduced power density of the reactor core (down to 69 kW/l). This factor enhances the operability of the fuel.

2.5. Automatic shutdown systems (4.2.3)

The automatic shutdown system is designed to generate signals and to execute commands for reactor power limitation, or reduction, or for shutdown, in any accidents caused by failures in the reactor plant or by errors of the plant personnel. The following types of layered or staged commands up to the emergency protection level act upon the control rods:

- prohibition of control rod upward movement (2nd type of preventive protection);
- drop of one or several control rod banks to the lowest position (1st type of preventive protection);
- drop of all control rods to the lowest position (emergency protection).

The reactor emergency protection is actuated by de-energization of the CRDMs. Signals initiating the emergency protection actuation are generated from one of two instrumentation sets using a "2 out of 3" logic. The signals are derived from the following parameter deviations:

- decrease of the reactor period;
- increase of neutron flux;
- stop of three RCPs;
- reactor pressure increase;
- reactor pressure decrease;
- coolant level lowering in the reactor;
- rise of pressure in the guard vessel;
- pressure increase in the containment;
- pressure drop in the main steam line;
- feedwater pressure decrease.

All control inputs and operator actions preventing the emergency protection operation are interlocked following the emergency protection actuation.

The emergency residual heat removal system is connected in response to emergency protection signals.

In addition, the reactor can be shut down by de-energizing the CRDMs through self-actuated devices responding to direct action of the pressure in the reactor or in the guard vessel, as well as by activation of the emergency boron injection system from the control system, or following rupture of the membrane.

2.6. Normal heat removal (4.2.3.4)

Normal cool down of the reactor is carried out through the SGs with dumping of steam, steam-water mixture and water to the processing condenser. The rate of reactor cool down is 30°C/h.

When the coolant temperature has been reduced to 130-150°C, the reactor residual heat can be removed also by the repair cooling system which provides for the reactor heat removal at refuelling. This system is made of two trains (2x100%) and is provided with a reliable power supply from the diesel generators. It might thus be used also in beyond-design basis accidents.

2.7. Emergency heat removal (4.2.3.5)

Emergency heat removal is provided through the built-in heat exchangers/condensers, through the intermediate circuit to the water storage tanks of the system's heat exchangers units, and by water evaporation from these tanks. Following dry-out of the tanks, the residual heat is dumped through the air heat exchangers. The system trains are completely independent from the SGs. The system is also used to remove residual heat after primary circuit loss-of-integrity accidents.

The system is actuated by opening the valves in the water HX's drain line in response to signals of the automatic control system, or through the self-actuated devices. The valves are powered from reliable power sources, including batteries.

2.8. Reactor coolant system integrity (4.2.3.6)

The low neutron fluence to the RPV, owing to the integral design of the reactor, removes the problem of its radiation embrittlement. Due to this fact there is no need of using surveillance specimens in the reactor.

Materials subjected to radiation wear are not used in the design. The leak-before-break criterion is realized. Elimination of large diameter primary system pipelines, use of flow restrictors in pipelines of supporting systems, and the arrangement of all piping in the upper part of the RPV, exclude both large and medium LOCAs.

Cold water jets impinging upon the RPV are excluded thanks to the absence of large-capacity water injection systems.

Multilevel overpressure protection system is provided for the reactor (see section 2.2).

Primary system strength is provided with margin for anticipated internal and external design loads.

Primary system integrity is ensured by testing and checks made during component manufacture and erection, and during operation of the plant.

Necessary inspections and tests of the RPV material and weldments are envisaged using NDT techniques.

SG leak-tightness is controlled by monitoring the secondary side coolant radioactivity.

The certified materials used in the design have been verified by long-term operational experience in VVER and marine propulsion reactors.

2.9. Confinement of radioactive material (4.2.3.7)

The limitation of release of radioactive products under normal and emergency conditions is provided by maintaining the integrity of all available protective barriers: fuel, cladding, RPV, guard vessel, and containment.

As this function is concerned, the following features of the design are important:

- leak-tight primary system, including the reactor coolant pumps, the closed primary coolant purification system and the boron control system;
- a guard vessel designed for the maximum pressure arising after a primary system loss of integrity. The guard vessel represents a leak-tight steel shell fabricated in machine-building works. Another function of the guard vessel is to keep the coolant level above the core;
- multi-sectional SGs designed for the primary pressure (up to the localizing valves);
- three isolation/localizing valves of different types installed on the SG in series which are actuated automatically by the direct action of the medium or by remote operation;
- availability of a pressure barrier in the systems for emergency residual heat removal, and for the primary system equipment cooling.

2.10. Protection of confinement structure (4.2.3.8)

The guard vessel as a localizing barrier is designed for the pressures arising after design-basis and beyond design-basis accidents, and for impacts of missiles and of coolant jets. It is equipped with a filtered discharge means and a heat removal system.

The guard vessel is protected against external impacts (aircraft drop, shock wave etc.) by the containment which is designed for such effects. The containment, guard vessel and localizing valves are designed for seismic impacts of magnitude 8 of the MSK-64 earthquake scale.

2.11. Monitoring of plant safety status (4.2.3.9)

The design envisages monitoring, diagnosis and presentation of information on all the systems important to safety in the most convenient form to the operator. Monitoring of the plant safety status can be carried out from the MCR and from the standby control board. In the plant status monitoring system special attention is paid to actuation and operation of the safety systems, presentation of unambiguous and clear information to the operator allowing him to back-up, if necessary, the automatic system actions.

An advisor system is provided for the operator, giving him recommendations for the identification and prevention of emergency situations and for taking the plant out of operation.

2.12. Preservation of control capability (4.2.3.10)

For preservation of the plant control capability in the event of MCR loss (due to fire or any other reason) a standby plant control board is provided which allows to shut the reactor down, to control its subcritical state, and to actuate the residual heat removal and localizing systems. This board is arranged in a significant distance from the power unit and is protected against external impacts (aircraft, shock wave, etc.).

In addition, local control boards are provided which do not require interaction with the MCR or with the standby plant control board.

2.13. Station blackout (4.2.3.11)

In the event of a station blackout a reserve power supply system is provided to ensure the operation of the systems important for safety. This power supply system consists of two trains of 100% capacity each. Reliable DC power supply is provided from accumulator batteries for the MCR, the standby plant control board and for the controlling safety systems for a period of 72 hrs.

The passive safety systems adopted for the design function normally under blackout conditions without electricity consumption, maintaining the safe state of the plant with no need for personnel intervention for a period of at least 3 days. The availability of self-actuated devices ensures putting the safety systems into operation under conditions of station blackout and failure of electrical control systems.

Automatic start-up of the diesel generators is not required, they are started remotely.

2.14. Control of accidents within the design basis (4.2.3.12)

After actuation of the safety systems an intervention of the plant personnel is prohibited for 10-30 min. This approach allows to eliminate erroneous actions by the personnel in the initial period of an accident when the plant parameters vary quickly. Then, the operating personnel may interfere and take the necessary actions according to the operating manuals.

For the plant personnel to make decisions a complete information on the course of an accident is available:

- radiation level;
- control rod position;
- status of the systems and components important for safety;
- status of the protective and localizing safety systems.

The plant specific features ensure an ample time reserve to evaluate the situation and to interfere, if necessary, in an accident (both design and beyond design) in case the automatic safety systems fail to function.

In the case that the plant personnel does not act, safety is provided nevertheless by the startup of the safety systems through the self-actuated devices.

2.15. Mitigation and control of severe accidents

The plant self-protection features and the availability of passive safety systems ensure an ample time reserve, amounting to hours or even days, in the case of an accident with failure of mitigating systems and equipment.

Accident control means are provided including systems for normal operation and special systems to prevent core damage.

Slow dynamics of transients, absence of threshold effects, and ample time reserve ensure an effective intervention during the course of an accident and mitigation of related consequences.

The capability to confine corium inside the reactor vessel or in the guard vessel is being validated in the design for postulated accidents with reactor core melting. Taking into account the plant specific features results in an effective in-reactor convection, in reduced heat loads from the corium to the RPV, and in an intensive heat removal from RPV outer surface at high pressure in the GV.

3. EXTENDED DATA LIST

Station output

Rated thermal power of the reactor	1800 MWt

Fuel assembly

Array	triangular
Number of fuel rods	287
Number of guide tubes for absorber/in-core instrumentation	18/1
Number of burnable poison rods with fuel	24
Fuel rod, length	3.895 m
outside diameter	9.1 mm
cladding material	zirconium alloy
cladding thickness	0.65 mm
initial internal pressure (He)	1.75 - 2.25 MPa
Fuel pellet, material	UO_2
density (percentage of theoretical density)	94.5%

Reactor core

Number of fuel assemblies	151
Active height	3.53 m
Equivalent diameter	3.04 m
Rod cluster control assemblies absorber	B_4C
Number of assemblies	139
Absorber rods per assembly	18
Fuel enrichments, first core	1.0, 3.6, 4.0, 4.4%
reload	4.0, 4.4%
(H_2O/UO_2) volume ratio	2.0
Average fuel burnup	up to 52 MWd/kg
Total weight of UO_2	62.1 t
Refuelling interval	1.5 - 2 years
Heat transfer surface in core	4465 m^2
Average fuel linear heat rating	108.0 W/cm
Average core power density	69.4 kW/l

Reactor Coolant System

Design conditions:	
- pressure	18.0 MPa
- temperature	350°C
Operating conditions:	
- pressure at core inlet	15.87 MPa
- pressure at steam generator outlet	15.7 MPa
- coolant temperature, vessel inlet/outlet	294.8/325°C
- flow rate	10210 kg/s

Reactor

Overall height (with reactor coolant pumps)	33.80 m
Outside diameter / support ring	5.97 / 6.13 m
Mass, dry/in operating status	2040 / 2240 t

Reactor vessel

Overall height with/without the head	23.96 / 20.76 m
Inside diameter	5.44 m
Wall thickness (opposite core)	265 mm
Mass (without head)	880 t
Material (forged rings)	heat resistant steel of VVER-1000 type
Design pressure/temp	18.0 MPa/350°C
Neutron fluence for service life	$7.5x10^{16}$ n/cm^2

Reactor coolant pump

Type	centrifugal, canned
Number	6
Design pressure/temp.	18.0 MPa/350°C
Design flow rate	8400 m^3/h
Pump casing material	stainless steel
Speed	1500 rev/min
Power at coupling, cold/hot	2950/2320 kW
Mass	37 t
Coast down time	30 s

Steam generator

Type	once-through, vertical
Number	12 sections
Heat transfer surface	13930 m^2
Number of heat exchanger tubes	66400
Tube dimensions (diameter x wall thickness)	13.1 x 1.5 mm
Total height (tube)	3.8 m
Transport weight of section	25 t
Tube material	titanic alloy
Live steam pressure	6.38 MPa
Steam flow	3420 t/h
Steam temperature	305°C
Feed water temperature	230°C
Water volume on secondary side	13.3 m^3
Total weight	180 t

Pressurizer

Total volume	80 m^3
Operating pressure, total/steam	15.7/11.8 MPa
Design pressure/temp.	18.0 MPa/350°C
No heaters	
Outside/inside diameter	5.97/5.44 m

Guard vessel

Material	steel
Gross volume	1440 m^3
Pressure (design)	4.0 MPa
Height/diameter (max.)	36.51 / 11.0 m
Design leak rate	0.15% of full volume during 24 h

Containment

Configuration (single or double)	single
Material	un-reinforced concrete
Gross volume	60000 m^3
Pressure (design)	0.2 MPa
Height/diameter	60.25 / 40 m
Design leak rate	0.3% of full volume during 24 h

REFERENCES

[1] General safety regulations for nuclear power plants (OPB-88), Gosatomnadzor, USSR Moscow, Energoatomizdat, 1990.

[2] Nuclear safety rules for reactors of nuclear power plants Moscow, 1990

BASIC INFORMATION ON DESIGN FEATURES OF THE PIUS NUCLEAR PLANT

TOR PEDERSEN
ABB Atom AB,
Västerås,
Sweden

Abstract

The paper describes the PIUS nuclear power plant design of ABB Atom, Sweden. The paper consists of three parts: - a general description of the plant concept; - a description of how the plant compares with the safety principles of INSAG-3 for 15 selected design areas; and - an extended data list. The general description outlines the basic design objectives and safety philosophy, describes the main features of the reactor plant and its safety systems, and discusses safety analysis and evaluation of accidents and incidents, including beyond-design accidents. The second part discusses plant performance in the areas of: - plant process control systems; - automatic safety systems; - protection against power transient accidents; - reactor core integrity; - automatic shutdown systems; - normal heat removal; - emergency heat removal; - reactor coolant system integrity; - confinement of radioactive material; - protection of confinement structure; - monitoring of plant safety status; - preservation of control capability; - station blackout; - control of accidents within the design basis; and - mitigation and control of severe accidents. The third part, finally, presents data related to the power plant as a whole, data on reactor core and fuel, on the reactor coolant system, the reactor pressure vessel, coolant pumps, steam generators and pressurizer, and on the containment.

1. GENERAL DESCRIPTION

1.1. Basic design objectives and safety philosophy

In recent years, a number of compelling arguments have been given for furthering the development of the established light water reactor technology to make it better adapted to future needs. Simplifications, improved economy and a "good neighbour" image represent three such aspects, which may well be seen as the most important ones. Early nuclear power plants were designed to be straight forward and simple, subjected to only very general formal requirements. As new safety concerns developed, regulatory bodies responded by issuing new requirements and guidelines, however, and these escalating formal requirements have resulted in a plethora of add-on safety features in present day nuclear power plants.

The increased number of systems and components, and associated increases in building volumes, have resulted in significant cost increases, but above all it implies that nuclear safety tends to be relying on complex interactions of a multiplicity of systems and equipment. And this complexity, in turn, makes analyses and evaluations take a long time; a large portion of the long construction periods, experienced in some countries, are probably due to this. Besides, the complex safety structure is very difficult to understand for anybody who is not familiar with the design, and it leaves ample room for possible human mistakes.

The PIUS concept represents an effort to accomplish a simplified reactor design which can be more easily understood by the general public. The basic design objectives that were established by ABB Atom at the start of the development work on SECURE, its heat only reactor design, encompassed:

- It should be competitive in small and moderate capacity units with respect to costs, availability and maintainability;
- It should be based on demonstrated widely employed basic technology to a maximum extent;
- It should be simple and flexible to operate and not make excessive demands on the resources of qualified personnel;
- The safety should be "transparent", ie., understandable to educated laymen, built on simple natural laws, and independent of failure-prone systems and components;
- It should be operator forgiving, i.e., the "human factor" as a risk element should be largely eliminated by design;
- It should be safe enough to be located almost anywhere, even in densely populated areas (from a technical point of view);
- It should be capable of surviving extreme external conditions without risk of environmental radioactive contamination.

These design objectives were carried over to the work on the power reactor PIUS, basically a pressurized water reactor (PWR) in which the primary system has been rearranged in order to accomplish an efficient protection of the reactor core and the nuclear fuel by means of thermal-hydraulic characteristics, in combination with inherent and passive features, without reliance on operator intervention or proper functioning of any mechanical or electrical equipment. Together with wide operating margins, this should make the plant design and its function, in normal operation as well as in transient and accident situations, much more easily understood and with less requirements on the capabilities and qualifications of the operators.

1.2. Design description

PIUS is a 600 MWe passive and simplified PWR, based on well established LWR technology and infrastructure. As noted above, its primary system configuration differs from traditional PWR designs, reflecting the goals of achieving increased simplicity and safety, in particular with respect to protection of the reactor core in possible accident scenarios. The basic arrangement is outlined in Figure 1-3, and a main flow diagram is shown in Figure 4.

The reactor core is an open PWR type core, located near the bottom of the highly borated reactor pool, contained in a prestressed concrete vessel cavity. The PIUS reactor does not use control rods, neither for reactor shutdown nor for power shaping. Reactivity control is accomplished by means of reactor coolant boron concentration control (chemical shim) and by coolant (moderator) temperature control. In comparison with current PWR practice, the core data are significantly relaxed in terms of average linear heat load, temperatures, flow rates and associated pressure drops. Power shaping at the beginning of an operating cycle and reactivity compensation for burnup are accomplished by means of burnable absorber (gadolinium) in fuel rods. This means that the boron concentration can be kept at a rather low level, throughout the operating cycle, and the moderator temperature reactivity coefficient will be strongly negative under all operating conditions.

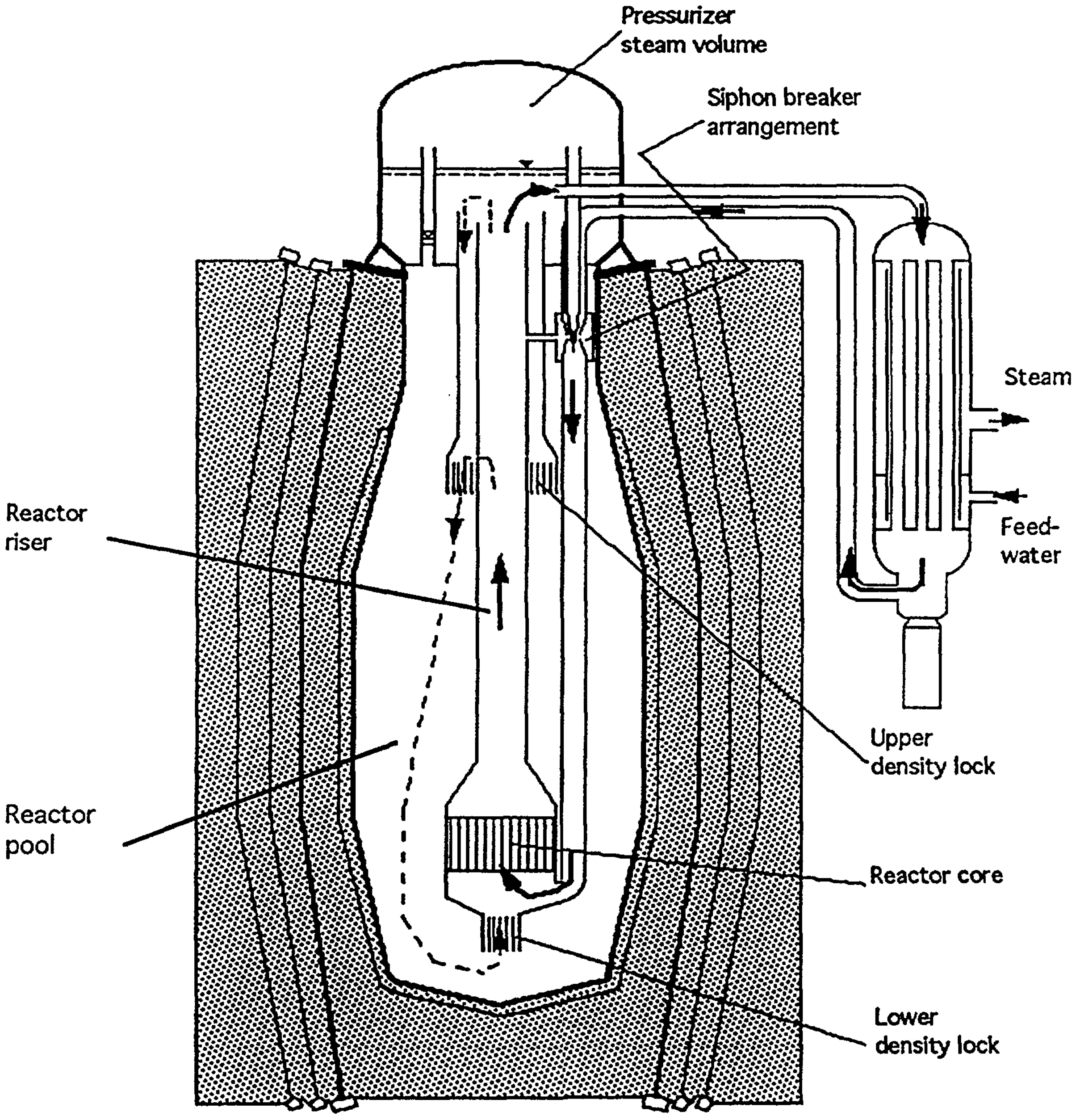


Fig. 1: PIUS - principle arrangement

From the core the heated coolant passes up through the riser pipe, leaves the reactor vessel through nozzles in its upper steel part, and continues in hot leg pipes to four straight tube once-through steam generators (Fig. 3). The main coolant pumps are located below the steam generators, and structurally integrated with these. The pumps are sized-up versions of the glandless, wet motor design pumps that are utilized as recirculation pumps in the ABB Atom BWR plants. The cold leg piping enters the reactor vessel at the same level as the hot leg nozzles, and the return flow is directed downwards to the reactor core inlet via the downcomer. On its way down, the flow velocity is increased in a siphon breaker arrangement with open connections to the pressurizer. During normal operation, the siphon breaker does not affect the water circulation, but in hypothetical cold leg rupture situations it will help minimize the loss of reactor pool water inventory. At the bottom of the annular downcomer the return flow enters the reactor core inlet plenum.

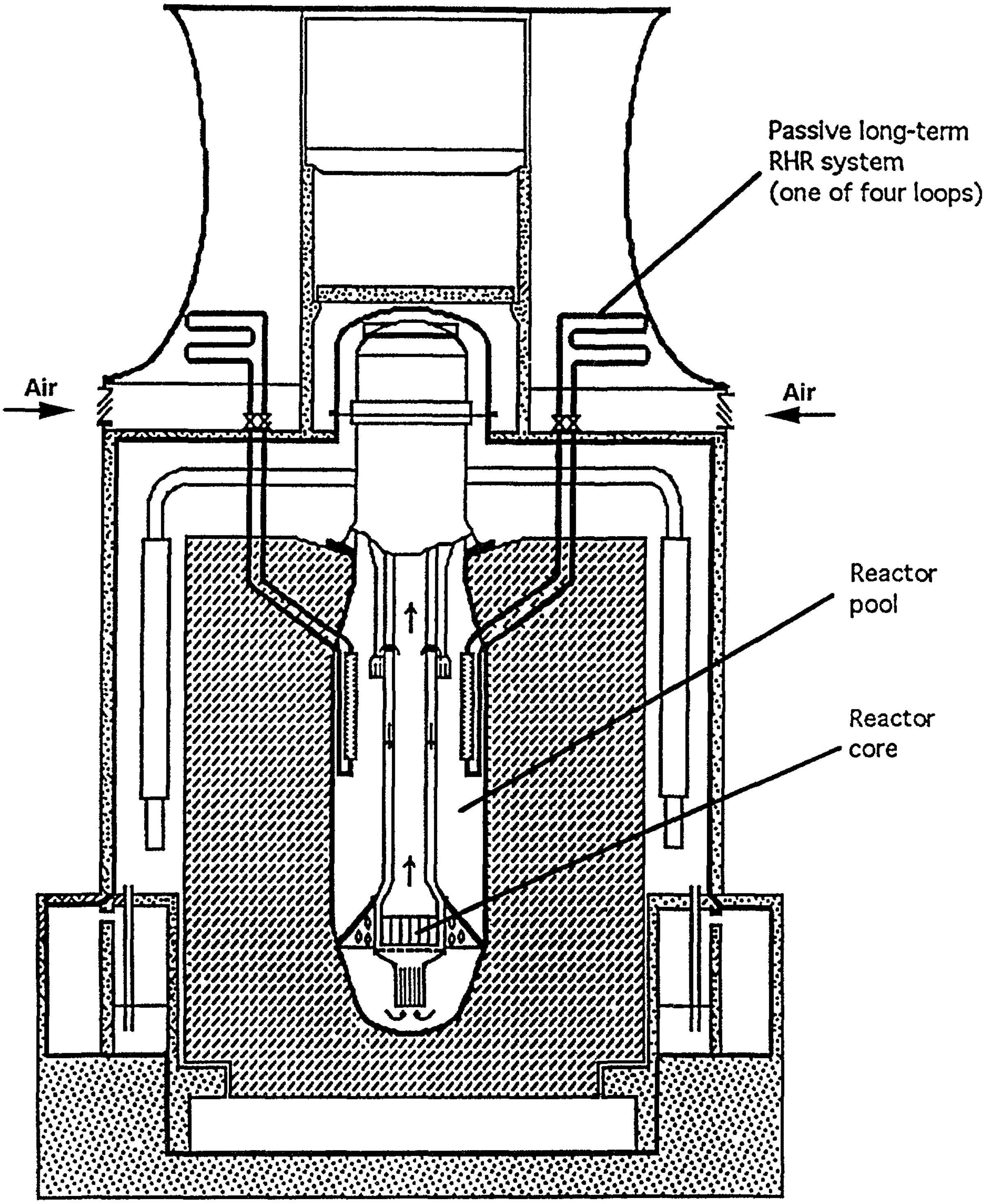
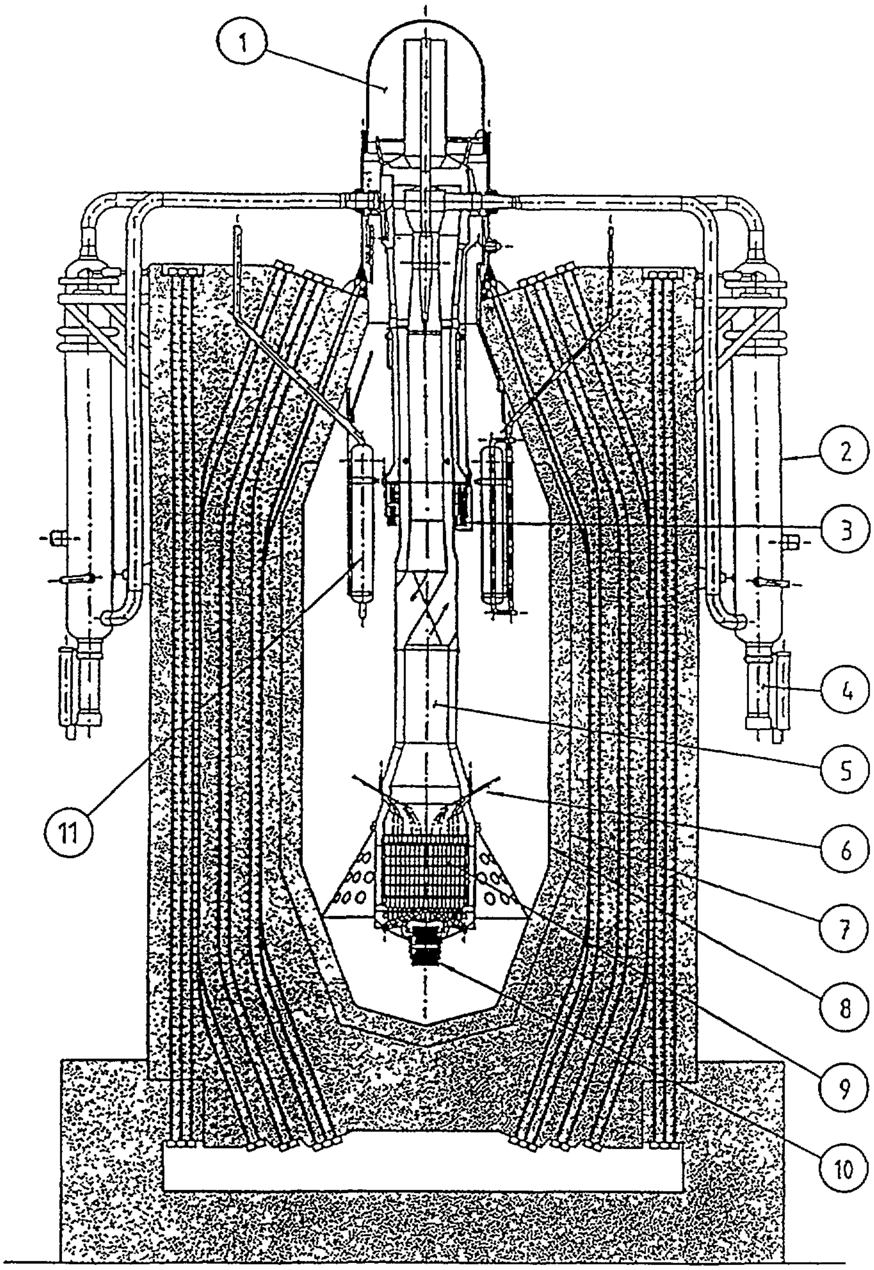


Fig. 2: PIUS - safety-grade structures

Below the core inlet plenum there is a pipe opening (less than a meter in diameter) towards the surrounding reactor pool. The pipe encloses a set of tube bundles to minimize water turbulence and mixing and ensure stable layering of hot primary loop water on top of colder reactor pool water. This pipe, with the tube bundles and the stratified water, is called the lower "density lock". The position of the interface between hot and cold water is determined by temperature measurements, and this information is used for controlling the main coolant pumps speed (or flow rate). The upper portion of the density lock pipe is normally filled with hot primary loop water, serving as a buffer volume to prevent ingress of pool water and spurious reactor shutdowns at minor operational disturbances. There is another "density lock" arrangement at a high location in the pool, connected to the upper riser plenum - the volume on top of the riser from which water is drawn into the hot leg pipes. This upper density lock has a similar arrangement of tube bundles and a buffer volume above the hot/cold water interface level. There are also a number of small openings directly from the riser to the density lock.



1. Pressurizer steam volume
2. Steam generator (4)
3. Upper density lock
4. Main coolant pump (4)
5. Riser
6. Core instrumentation
7. Embedded steel membrane
8. Pool liner
9. Core
10. Lower density lock
11. Submerged pool cooler, cooled in natural circulation by ambient air.

Fig. 3: PIUS - principle features of NSSS

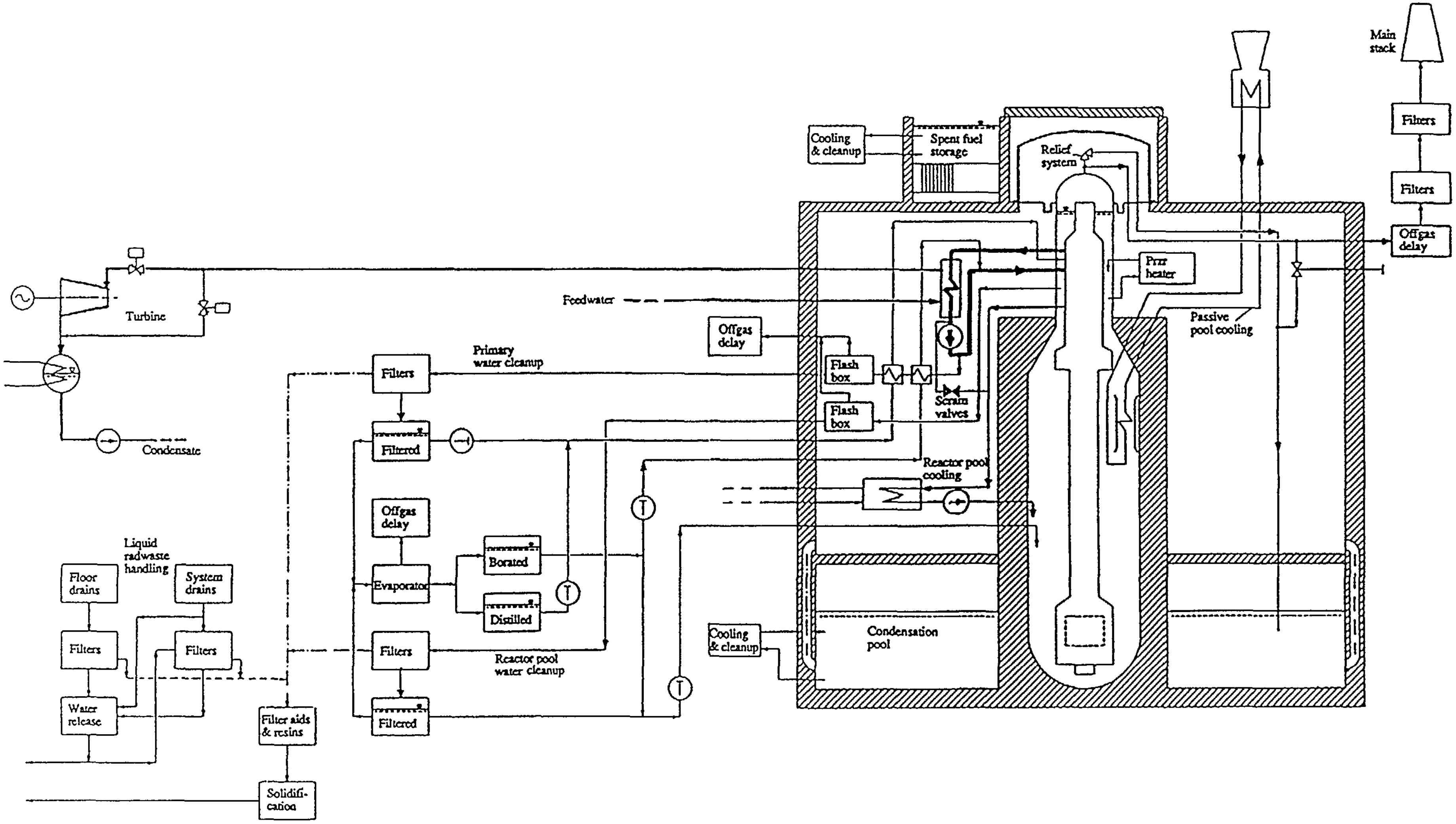


Fig. 4: PIUS - main flow diagram

This PIUS reactor system configuration - with the two always open density locks - is the basis for an exceptional safety performance. An open natural circulation path through the core is always present - from the reactor pool to the lower density lock, to the core via inlet pipes, through the core itself, the riser, the passage from the upper riser plenum and through the riser-density lock connections, and the upper density lock back to the pool.

In a PIUS plant, the core coolant flow rate is determined by the thermal conditions at the core outlet - relative to the reactor pool. The resulting pressure drop across the core and up through the riser must correspond to the static pressure difference between the interface levels in the upper and lower density locks. During normal plant operation, the speed of the main coolant pumps is controlled in such a way that there is a pressure balance across the lower density lock; this way, the hot/cold interface in the lower density lock is maintained at a constant position, and the natural circulation circuit is kept inactive. In case of a severe transient or an accident, the pressure balance is lost and the natural circulation flow loop will be established, providing both reactor shutdown and continued core cooling.

As long as the position of the interface level in the lower density lock is kept constant, the hot/cold interface level in the upper density lock is determined by the total volume of the primary loop water mass. The interface level position measurements in the upper lock are basically used for control of the reactor pool volume. The reactor primary loop volume control utilizes level measurements in the pressurizer.

The reactor pool water is continuously heated by heat losses from the sub-merged hot parts of the primary system. In order to keep losses at an acceptable level, the hot parts are provided with a thermal insulation, a wet metallic type insulation, consisting of a number of parallel, thin stainless steel sheets with stagnant water between them. The reactor pool water is cooled by two systems; one with forced circulation of pool water through out-of-vessel heat exchangers and pumps, and one entirely passive system utilizing coolers submerged in the reactor pool and natural cooling water circulation loops up to dry, natural draft cooling towers located on top of the reactor building. The passive system (Fig. 5) ensures the cooling of the reactor pool in accident, and station blackout, situations, and prevents boiling of the reactor pool water inventory. In the hypothetical case that all pool cooling systems fail, the water inventory ensures the core cooling for a protracted period of time (7 days).

The prestressed concrete vessel (Fig. 3) encloses a cavity with a diameter of about 12, and a depth of about 38m. The concrete vessel proper is a monolithic structure that is anchored to the foundation mat by means of prestressing tendons. The pressure retaining capability of the vessel is ensured by a large number of prestressing tendons - partly horizontal tendons run around the cavity, partly vertical tendons run from the top to the bottom, - and by reinforcement bars. The cavity is provided with two leaktightness barriers; on the inside, an internal stainless steel liner, and, about 1 m into the concrete, an embedded steel membrane - up to a level above the upper density lock to ensure that the reactor pool water volume below this level cannot be lost by liner leakage. Concrete vessel penetrations are not permitted below this level.

On top of the prestressed concrete vessel there is a steel vessel extension which is fixed by means of separate tendons anchored to the bottom of the concrete vessel. This extension contains pipe nozzles for the hot and cold leg pipes, the forced circulation loops of the reactor pool cooling system, and some other system pipes. It also encloses the upper riser plenum, and the pressurizer.

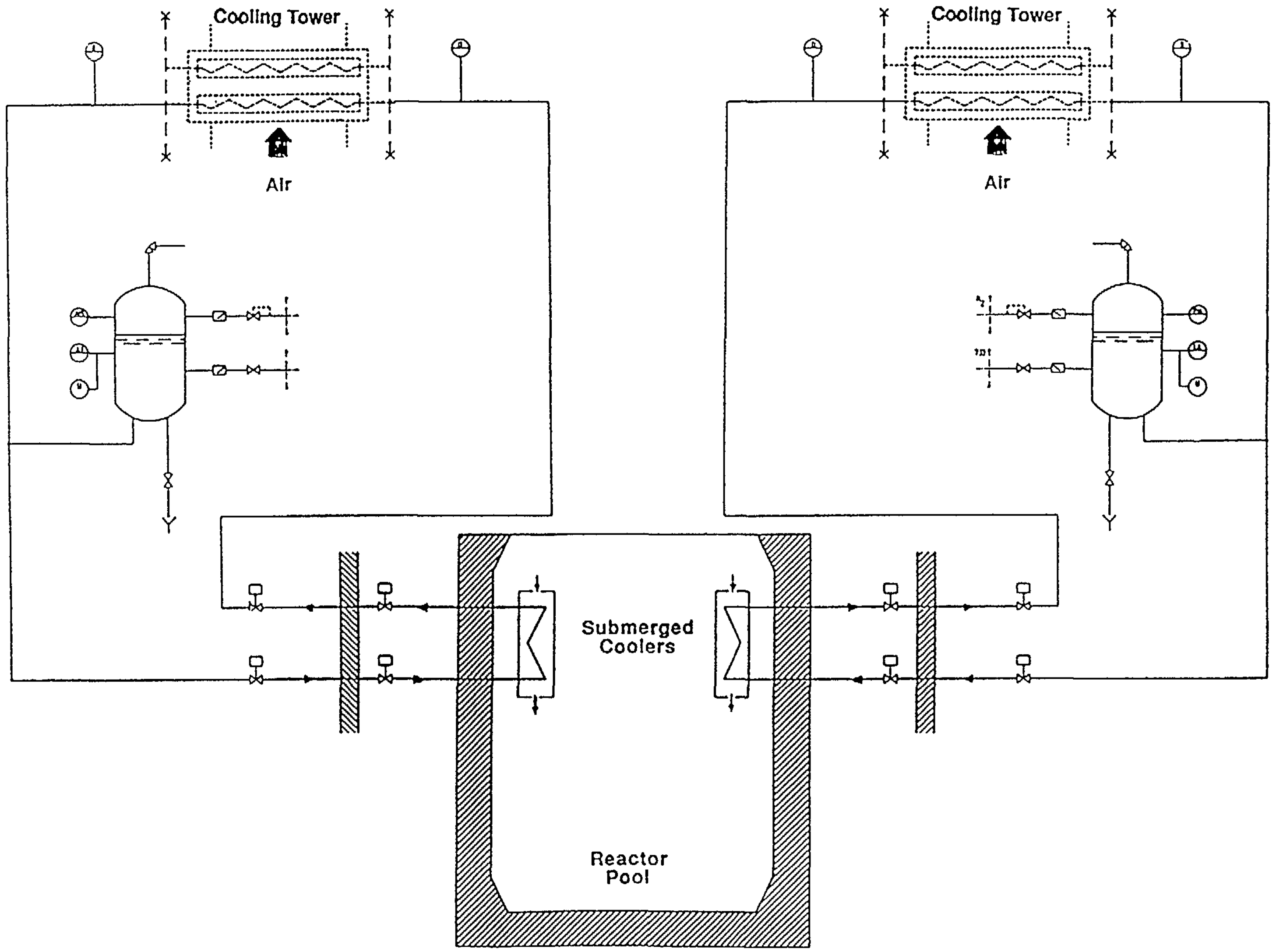


Fig. 5: PIUS - passive closed cooling system for heat removal from reactor pool

The reactor system is pressurized by means of steam supplied from an electrically heated boiler that draws water from the pressurizer water pool. The pressurizer steam volume is comparatively large and, together with its volume of saturated water, the reactor system can accommodate pressure and level variations that may occur during operational transients and accident situations. The pressurizer is connected to the reactor pool via funnels up into the steam volume, and to the reactor primary loop via open passages from the pressurizer "pool".

The reference turbine plant design for the PIUS plant design, is similar to that of present-day LWR plants. The PIUS NSSS steam data (270°C at 4.0 MPa) is inferior (lower) compared with the steam supplies from standard present-day LWR plants, and therefore PIUS requires a somewhat larger size turbine than other modern LWR plants. The nominal power output of the turbine unit will be 635-665 MWe depending on the site conditions.

The plant layout features four separated blocks of main buildings (Fig. 6) which help shortening the construction schedule. The plant has one entrance only for daily use, backed up by an emergency exit. The reactor building, basically a cylindrical structure with a diameter of about 60 m and a height of about 70 m makes up the main block. Vertical shafts are arranged on two diametrically opposite sides of the "cylinder", up to one of the reactor service room aisles. One of these shafts is the transport shaft from the ground level, eg., for fuel transport to/from the plant; the other provides communication with the adjacent control building.

The reactor service room at the top of the building has a second aisle, perpendicular to the first one. The natural-draft cooling towers for the long-term passive RHR system are located in the quadrants between these reactor service room aisles; the four cooling towers are physically protected by the reactor service room structures. All safety-grade systems are located within the reactor building which encloses the containment, the fuel handling equipment, the fresh fuel storage, the spent fuel storage pool and the emergency control room (the auxiliary shutdown facility) with associated instrumentation, control equipment, and batteries for electric power supply.

The second block includes the reactor auxiliary and waste management building, housing the reactor water cleanup system and the liquid and solid radwaste systems, the radioactive maintenance shops, housing the active workshop, and storage rooms for potentially radioactive waste. This building complex is situated on one side of the reactor building, and physically interconnected with it by pipe culverts, and also by the shared transport air lock. The control building, with the main control room, computer rooms, personnel entrance, etc., and the diesel generator and non-vital low voltage switchgear building make up the third block. The fourth block, finally, is formed by the turbine building, the non-vital medium voltage switchgear building, the transformer enclosures, the service water pump house and the circulating water pump house. This block is located on the other side of the reactor building, compared with the second block.

The layout is divided into clean and potentially contaminated areas with directional ventilation, where air from potentially contaminated areas could leak to cleaner areas. Filtered ventilation by way of the stack is available for potentially contaminated rooms when needed. Electrical systems and process systems are separated from each other and located in different rooms and culverts. Process systems are similarly split into radioactive or non-radioactive systems.

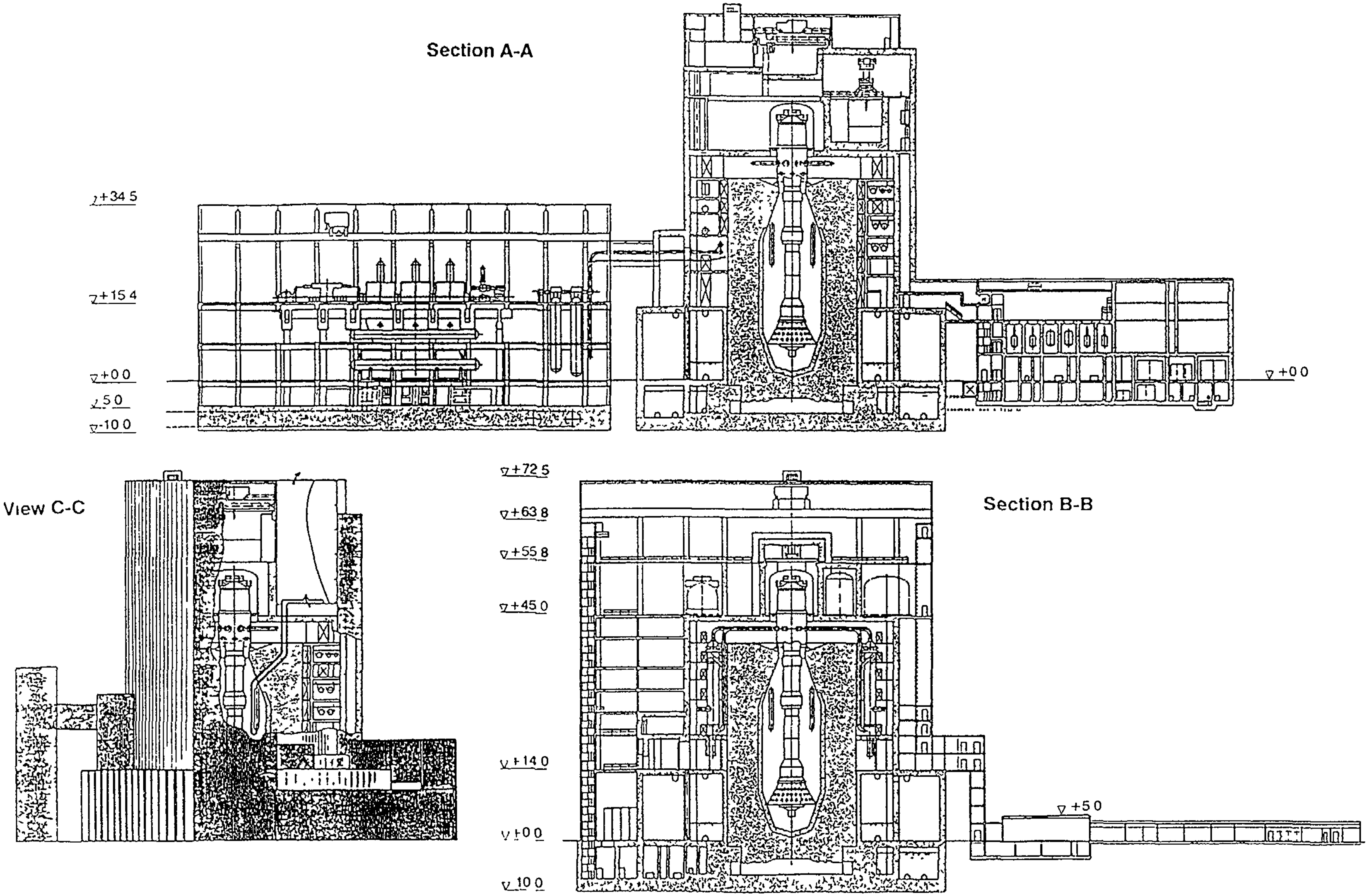


Fig. 6: PIUS - general building arrangement

Only the systems that are part of the high pressure reactor coolant system are located within the containment. Systems carrying hot pressurized reactor water are not allowed to extend beyond the containment. The reactor water cleanup and the liquid and solid waste handling systems are located in a separate building with concrete walls for separation and shielding of major components. Most of the systems and components are therefore installed in areas with more or less unrestricted access, for maintenance, inspection and service. Transport routes for equipment and communication routes for personnel, as well as adequate space around the equipment, are important considerations in the layout and installation activities.

In summary, PIUS is essentially a PWR that predominantly utilizes existing LWR technology. Major differences compared with current LWR plant designs are limited to the areas of thermal-hydraulic arrangement; the use of density locks (thermal barriers), siphon breakers, and wet thermal insulation; the pressure vessel of prestressed concrete; the implementation of a long-term passive residual heat removal system; and reactivity control without control rods. Main design parameters have been conservatively chosen; i.e. the core power density and linear heat rating are lowered; the power coefficient is negative throughout the operating cycle; and the reactor pressure and temperature are lowered as compared to present-day PWR plants

Protection against core degradation accidents is ensured by the laws of physics alone; intervention of active systems is needed to keep the reactor in operation, not for safety, to prevent it from reverting to a state of shutdown and natural circulation core cooling. Accident analyses performed so far confirm that the safety goals are fulfilled; no accident sequence leading to core degradation has been identified. The self-protective thermal-hydraulics have been successfully demonstrated in normal and under severe transient conditions. The remaining departures from current reactor technology listed above, except the absence of control rods, have been either verified through testing or have a sound basis in technology outside of reactor technology. The absence of control rods is actually an advantage since mechanical devices and interacting detector and insertion systems are eliminated. The risk of serious reactivity insertion due to control rod malfunctions is also eliminated. From a licensing point of view, the concrete vessel and the absence of control rods represent important departures from current technology, but they are also, together with the totally passive safety systems, the key elements for the favourable safety performance.

Significantly fewer systems and components are needed in PIUS than in present-day LWR plants. Most important is that the self-protective functions of the reactor design have resulted in a substantial reduction in the number of safety-grade systems and components. The major portion of the systems and components are not safety-grade, which means that the need for in-service inspection and periodic testing, etc. has been significantly reduced.

1.3. Safety analysis and evaluation of accidents and incidents

The safety analysis will be carried out in agreement with the US NRC Regulatory Guide 1.70 - *Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants* and following the guidelines reported in NUREG 0800 - *Standard Review Plan.*

The analyses and evaluations of accidents and incidents will cover the following event categories, as applicable to the PIUS design:

i) Increase in heat removal by the secondary system
ii) Decrease in heat removal by the secondary system
iii) Decrease in reactor coolant system flow rate
iv) Reactivity and power distribution anomalies
v) Increase in reactor coolant inventory
vi) Decrease in reactor coolant inventory
vii) Anticipated Transient Without Scram

In this context it should be noted that the traditional chapter 15 of the Safety Analysis Report which deals with Accident Analysis will be supplemented by a chapter addressing Response to Severe Accidents and Source Terms.

The plant response to the different Design Basis Events, the initiating events listed in Regulatory Guide 1.70 and NUREG-0800, is analyzed and evaluated in accordance with the rules stipulated by the regulatory body; e.g., application of the single failure criterion, assuming an operator "non-activity" period of at least 30 minutes, and taking functional credit only for safety-grade equipment and systems; the so-called design basis accidents refer to these events and the evaluation in accordance with conservative rules.

For obvious reasons, analyses of plant responses to accidents and incidents can not be limited to these "Design Basis Accidents"; the implications of further failures and malfunctions, in combination or simultaneous with, the initiating event, etc. need be assessed carefully. When analyzing such "beyond Design Basis Accidents", however, it is also quite obvious that the rules with respect to calculational methods, operating conditions, etc. can be less conservative; best estimate calculations based upon engineering judgements, and with credit taken for non-safety-grade equipment, should constitute an acceptable approach.

A tentative expansion of the above listing of incidents and accidents to be analyzed is presented below, consisting of both Design Basis and beyond Design Basis situations. The analyses and evaluations of these accidents and incidents will be based on calculations, comparisons and references as appropriate; methodologies, evaluation models and acceptance criteria for the analyses and categorization of Design Basis Events will be established at an early stage.

The expanded list comprises:

- Increase in heat removal by the secondary system due to:
  - decrease in feedwater temperature (by loss of last feed heater stage);
  - increase in steam or feedwater flow rate;
  - postulated steam line break inside and outside the containment, with scram initiation, and with failure to scram.
- Decrease in heat removal by the secondary system due to:
  - turbine trip;
  - inadvertent closure of main steam isolation valves, with scram initiation, and with failure to scram;
  - loss of normal feedwater flow, with scram initiation, and with failure to scram;

  - feedwater system pipe break;
  - loss of ordinary AC power supply to plant auxiliaries.

- Decrease in reactor coolant system flow rate due to:
  - trip of one reactor coolant pump (i.e., partial loss of forced coolant flow), with scram initiation, and with failure to scram;
  - trip of all reactor coolant pumps (e.g., resulting from loss of AC power supply)

- Reactivity and power distribution anomalies due to:
  - reduction in boron concentration, e.g., a malfunction in the Chemical and Volume Control System resulting in decreased coolant boron content, at low power level, and at high power level and with scram initiation and with failure to scram.

- Increase in reactor coolant inventory due to:
  - CVCS malfunction, with scram initiation, and with failure to scram.

- Decrease in reactor coolant inventory due to:
  - opening of pressure relief valves, with scram initiation, and with failure to scram;
  - pipe rupture upstream pressure relief system valves, with scram initiation, and with failure to scram;
  - steam generator tube rupture
  - double-ended guillotine break in one line of the forced pool cooling system, with scram initiation, and with failure to scram;
  - medium break in cold leg, at high location and at low location, with scram initiation, and with failure to scram;
  - double-ended guillotine break in cold leg, at high location, and at low location;
  - double-ended guillotine break in hot leg, at high location, with scram initiation, and with failure to scram.

With respect to responses to severe accidents that would give rise to significant releases of radioactive products, e.g., post-core-melt situations, no analyses have been performed yet, since no accident sequence leading to a core degradation situation, with significant fuel damage, has been identified; the plant response analyses show that the PIUS design is extremely robust with very large margins.

2. DESCRIPTION OF 15 SPECIFIC DESIGN AREAS AS SELECTED FROM INSAG-3

In the following sections the reference to INSAG-3 has been put in parentheses after each heading.

2.1. Plant Process Control Systems (4.2.2.1)

Principle 121 of INSAG-3 states that "Normal operation and anticipated operational occurrences are controlled so that plant and system variables remain within their operating ranges. This reduces the frequency of demands on the safety systems."

As noted in the design description above, proper speed control of the reactor coolant pumps is fundamental for the operation of PIUS; the coolant flow rate from the pumps must match the "natural circulation" coolant flow rate through the core and up the riser. The control requirements are still rather modest with respect to both accuracy and response time, due to the "buffer volumes" in the density locks.

The reactor power is controlled by the boron content and temperature of the reactor coolant. During normal plant operation, the power is controlled without adjustment of the boron content in the reactor coolant, utilizing the strongly negative moderator temperature reactivity coefficient. A power change is accomplished by simply adjusting the feedwater flow rate or the steam flow rate. A secondary side flow rate increase results in a cool-down of the return flow to the reactor, a lowered average moderator water temperature and thus an increase in reactor power. This procedure is applied over a 40% power range with a 20%/min rate of change in plant power. Beyond this range adjustment of the boron content is needed in order to keep the reactor core coolant outlet temperature within acceptable limits. The boron content is controlled by injecting distilled water for power increase or high boron content water for power decrease, and withdrawing a similar amount of water, corresponding to the procedures in other PWR plants. The moderator boron concentration is used for slow reactivity changes and for establishing the upper limit of a reactor power control range. It is also used for rapid shutdown by opening scram valves that let borated reactor pool water into the primary loop at the coolant pump suction.

Apart from the reactivity control tasks, the chemical and volume control system (CVCS) of PIUS supplies the primary loop with cleaned, filtered makeup water and with chemicals for water chemistry control. The primary loop water volume is controlled by withdrawing primary loop water and conveying it to the reactor water cleanup system for treatment. The inlet and withdrawal rates are controlled in such a way that the water level in the pressurizer is maintained at a constant level. The reactor water cleanup system also serves to clean and control the reactor pool water; a certain amount of pool water is continuously withdrawn, treated in the cleanup system and re-injected into the pool, possibly with chemical additives. The ratio between in- and outlet flow rates is adjusted when needed to maintain the hot/cold water interface in the upper density lock at a nearly constant position.

On the secondary side, the steam flow rate to the turbine is controlled in accordance with a steam pressure profile, and the water supply to the steam generators from the feedwater pumps is controlled in such a way that the steam leaving the steam generator will have a certain minimum level of superheat.

2.2. Automatic safety systems (4.2.2.2)

Principle 125 of INSAG-3 states that "Automatic systems are provided that would safely shut down the reactor, maintaining it in a cooled state, and limit any release of fission products that might possibly ensue, if operating conditions were to exceed predetermined setpoints."

The primary goal of nuclear safety, as reflected in the above principle, is to prevent radioactive matter from entering the environment and unprotected parts of the plant premises. The dominating part of such matter, and practically all volatile nuclides of real concern in this context, are located in the reactor fuel. Hence, protection of the core against overheating and damage is the top-level goal in reactor safety. In practice, this can be ensured by "*keeping the core submerged in water at all times, and keeping the rate of heat generation below the cooling capability of the surrounding water avoiding Departure from Nucleate Boiling (DNB)*". This has led to the PIUS design, with the large reactor pool in a prestressed concrete reactor vessel and the special reactor primary loop arrangement with always open connections to the borated water in the reactor pool. The Defence-in-Depth philosophy represents an important principle in nuclear safety strategies, and it is, of course, applied also to PIUS - with a significant shift in emphasis towards prevention/protection, and a corresponding relaxation with respect to requirements on accident management, in particular taking into consideration that so far no accident sequences leading to core damages have been identified.

An "ultimate" protection of the reactor core against overheating and fuel damage is provided by the unique PIUS arrangement - core submergence in the large pool of borated water, and transition to reactor shutdown and core cooling in a natural circulation mode without reliance on equipment for detection of off-normal conditions, initiation of actions, actuation of equipment, nor equipment relying on the displacement of mechanical bodies. PIUS is also provided with instrumentation, protection logic, and actuation systems for reactor shutdown, residual heat removal, containment isolation, etc. in a similar way as present-day LWR plants. Their importance for safety is significantly reduced, however.

Compared with current commercial LWR designs a number of safety-grade systems have been eliminated; control rods and the safety injection boron system are replaced by the density locks, an automatic depressurization system is not required, the auxiliary feedwater supply system for RHR is replaced by the reactor pool, containment heat removal and spray systems are replaced by the passive cooling of the reactor pool. Safety-grade closed cooling water systems, HVAC systems, and a.c. power supply systems have been replaced by non-safety-grade systems, allowing major simplification of the plant.

Remaining safety-grade functions are performed by the reactor protection system which initiates opening of the scram valves to achieve a reactor scram, the containment isolation system which initiates isolation of the containment by closing isolation valves, the reactor vessel safety valves based on pressure-activated components, and the passive reactor pool cooling function. These functions are not absolutely needed for the protection of the core, however.

2.3. Protection against reactivity transients (4.2.3.1.)

Section 4.2.3. of INSAG-3 discusses design features that serve specific safety functions, and Section 4.2.3.1 refers to "Protection against power transient accidents" - similar to the title of this specific design area. The associated Principle 148 states that "The reactor is designed so that reactivity induced accidents are protected against, with a conservative margin of safety".

As noted above, PIUS is essentially a PWR that predominantly utilizes existing LWR technology. Major differences compared with current LWR plant designs are limited to the areas of thermal-hydraulic arrangement; the use of density locks (thermal barriers), siphon breakers, and wet thermal insulation; the pressure vessel of prestressed concrete; the implementation of a long-term passive residual heat removal system; and reactivity control without control rods.

Main design parameters have been conservatively chosen; ie. the core power density and the linear heat rating are lowered; the power coefficient is negative throughout the operating cycle; and the reactor pressure and temperature are lower as compared to present-day PWR plants.

The reactor core is physically well protected by the enclosing containment structure and the thick-walled, strong concrete vessel walls. Protection against reactivity transients progressing to core degradation accidents is ensured by the laws of physics alone; intervention of active systems is needed to keep the reactor in operation, not for safety, to prevent it from reverting to a state of shutdown and natural circulation core cooling. The self-protective thermal-hydraulics have been successfully demonstrated in normal and under severe transient conditions. The remaining departures from current reactor technology listed above, except the absence of control rods, have been either verified through testing or have a sound basis in technology outside of reactor technology. The absence of control rods is actually an advantage since mechanical devices and interacting detector and insertion systems are eliminated. The risk of serious reactivity insertion due to control rod malfunctions is also eliminated.

Accident analyses performed so far confirm that the safety goals are fulfilled; no accident sequence leading to core degradation has been identified. In PIUS, intervention of active systems is needed to keep the reactor in operation, not for safety, preventing it from reverting to a state of shutdown and natural circulation core cooling.

2.4. Reactor core integrity (4.2.3.2)

Principle 151 of INSAG-3 states that "The core is designed to have mechanical stability. It is designed to tolerate an appropriate range of anticipated variations in operational parameters. The core design is such that the expected core distortion or movement during an accident wihin the design basis would not impair the effectiveness of the reactivity control or the safety shutdown systems or prevent cooling of the fuel".

As noted above, the average power density and the linear heat rating of the PIUS core are low compared to present-day PWR plants, the core height is much smaller, the dynamic pressure drop across the core is lowered; ie. the thermal and mechanical loads and stresses are lowered, and mechanical stability is not anticipated to represent any problem. The PIUS arrangement with the submergence in the borated water pool and the ever-present openings between the pool and the primary loop provide an effective assurance that reactor shutdown and decay heat removal will be ensured in almost any conceivable situation.

2.5. Automatic shutdown systems (4.2.3.3)

INSAG-3 principle 156 states that "Rapidly responding and highly reliable reactivity reduction for safety purposes is designed to be independent of the equipment and processes used to control the reactor power. Safety shutdown action is available at all times when steps to achieve a self-sustaining chain reaction are being intentionally taken or whenever a chain reaction might be initiated accidentally".

As noted to section 2.2. above, in PIUS an ever-present "ultimate" protection of the reactor core against overheating and fuel damage is provided by the unique arrangement - with the core submerged in a large pool of borated water, and transition to reactor shutdown and core cooling in a natural circulation mode without reliance on equipment for detection of off-normal conditions, initiation of actions, actuation of equipment, nor equipment relying on the displacement of mechanical bodies.

PIUS is also provided with instrumentation, protection logic, and actuation systems for reactor shutdown, residual heat removal, containment isolation, etc. in a similar way as present-day LWR plants. Their importance for safety is significantly reduced, however. The equipment of these instrumentation, monitoring, protection, and actuation systems is separated from that of other systems and located in separated compartments at the bottom of the reactor building. The reactor protection system (RPS), with a two-out-of-four coincidence logic, has the task of initiating power level reduction, reactor shutdown or reactor scram when reactor process parameters exceed set limits, in order to prevent further departure from permissible conditions.

In most cases, a runback to a lower power level, using the secondary side control, or going to hot standby or hot shutdown conditions by injecting high boron content water into the primary loop, will be an adequate countermeasure. A reactor scram is initated only in a few accident situations by opening the scram valves which will let borated reactor pool water into each of the cold legs at the suction of the coolant pumps. Borated water then reaches the core in a few seconds and shuts down the reactor to hot, subcritical conditions; primary loop structures will be subjected to a rapid cool down by some 50-60 K - a rather mild thermal transient and quite insignificant with respect to thermal fatigue.

The the scram valves system is considered safety-grade, even though the system function does not fully comply with the requirements on safety-grade systems; its successful function depends on continued operation, at least for a certain period of time, of the non-safety-grade main coolant pumps. However, whenever these pumps stop operating, the reactor will immediately be shut down by the self-protecting shutdown mechanism, - by the borated pool water ingressing through the lower density lock.

2.6. Normal heat removal (4.2.3.4)

Principle 159 of INSAG-3 states that "Heat transport systems are designed for highly reliable heat removal in normal operation. They would also provide means for the removal of heat from the reactor core during anticipated operational occurrences and during most types of accidents that might occur".

The normal way of heat removal from the primary loop in PIUS goes, as in other PWR plants, via the steam generators to the turbine plant, through the turbine unit to the main condenser.

When the power level is low, or when the turbine unit is not in operation, the steam may be routed directly to the main condenser via steam bypass (dump) valves.

If the condenser is not available, heat (steam) may temporarily be dumped to the condensation pool in the containment; most likely the reactor will be shut down in a controlled way - with heat removal to the heat sink via the reactor pool and its active cooling systems.

2.7. Emergency heat removal (4.2.3.5)

Principle 161 of INSAG-3 states that "Provision is made for alternative means to restore and maintain fuel cooling under accident conditions, even if normal heat removal fails or the integrity of the primary cooling system boundary is lost."

As noted in section 2.6. above, the normal emergency heat removal takes place via the reactor pool water; the primary loop heat is transferred to the pool water by the natural circulation loop through the density locks.

From the reactor pool the heat is transported to the ultimate heat sink by means of the active forced circulation cooling system and the cooling chain, or to the ambient air by means of the submerged coolers, the natural circulation cooling water loops and the natural draft cooling towers on top of the reactor building.

Some "Feed and bleed" procedures may also, to some extent, be used for emergency heat removal; heated reactor water can be withdrawn to the cleanup system and replaced with cold cleaned water; steam can be discharged to the condensation pool in the containment with supply of makeup water (eg. from the cleanup systems) to the primary loop or to the reactor pool.

2.8. Reactor coolant system integrity (4.2.3.6)

INSAG-3 principle 163 states that "Codes and standards for nuclear vessels and piping are supplemented by additional measures to prevent conditions arising that could lead to a rupture of the primary coolant system boundary at any time during the operational life of the plant."

As noted in the design description, the PIUS reactor coolant system is, with respect to the reactor coolant pressure boundary (RCPB), essentially similar to that of other PWR plants, except for the prestressed concrete reactor vessel (PCRV) that replaces the lower portion of the traditional reactor pressure vessel (RPV) made in steel.

The steel portions of the RCPB are designed and manufactured in accordance with the same rules that are applied to current PWR plants; this applies to the upper steel extension of the reactor vessel, the nozzles, the hot and cold leg piping, the steam generators and the reactor coolant pumps. The stipulations on in-service inspection and maintenance will also be closely the same.

Similar requirements apply to the PCRV; special attention is here paid to the condition and loading of the prestressing tendons, and to possible presence of leakages through the inner liner of the cavity at low locations. The space between the two leakage barriers is continuously monitored for leakages, either into it from the cavity or out of it through the embedded membrane.

The PIUS arrangement with the large pool of water ensures that a rupture of the primary coolant system boundary in almost any conceivable cases will have no catastrophic consequences; in the same way as for other PWR plants, the worst break is a large double-ended cold leg LOCA. The impact on the core and fuel is limited, however, and no fuel damages are anticipated. A catastrophic failure of the PCRV (at a low location) is very unlikely taken the double barriers, the large number of prestressing tendons, some 2x100% in capacity, and the conventional reinforcement with a pressure bearing capacity of some 70%.

The "normal" concern about neutron radiation of the RPV in the core belt region is no concern with PIUS; the distance between the vessel wall with the steel liner and the core is so large.

2.9. Confinement of radioactive material (4.2.3.7)

Principle 171 of INSAG-3 states that "The plant is designed to be capable of retaining the bulk of the radioactive material that might be released from the fuel, for the entire range of accidents considered in the design."

The PIUS nuclear steam supply system (the concrete vessel and the reactor system) is, in a similar way as in other LWR plants, enclosed in a large containment structure. The reference design containment is of the pressure suppression type. Blowdown pipes lead from the drywell into a large condensation pool in the wetwell. All equipment containing reactor loop or reactor pool water at high pressure and high temperature is located inside the containment which is designed to withstand a double-ended break of the largest pipe. The structure is made of reinforced concrete with a strength capable of resisting the impact of a crashing aircraft. The whole containment is provided with a steel liner in order to ensure leaktightness. A steel dome closes the shaft above the reactor vessel.

The containment structure is in turn partly enclosed in a reactor building (a secondary containment). Pools for storing spent fuel and reactor internals during refuelling are arranged in the reactor building, on top of the reactor containment. The portions of the reactor service room that contain the reactor cavity and the fuel pools are also designed with sufficient strength to provide protection against a crashing aircraft.

During refuelling operations the containment integrity is somewhat "disabled" since the containment dome and the reactor vessel head are removed. For refuelling, the cavity above the dome is filled with water, the reactor internals are then lifted out in sections, and placed in the water-filled cavity. Refuelling is carried out with a conventional refuelling machine from the reactor service room. Fresh fuel is brought into the cavity from a fresh fuel storage in the reactor building, and spent fuel is moved to an adjacent spent fuel pool at the reactor service room floor level.

The steam lines from the steam generators and the feedwater lines to them are provided with isolation valves inside and outside the containment wall - the outer valves being located in a separate protected compartment. The pressure relief valves on the steam lines blow to the condensation pool inside the containment, as do the pressure relief valves of the reactor pressure vessel.

As noted in the design description, the upper portions of the reactor building, which constitute the physical protection for the reactor cavity and the spent fuel storage pool, and the reactor containment, is designed to withstand the impact of a crashing airplane. The reactor building complex, including the enclosed reactor containment and the safety-grade equipment, is designed against the effects of earthquakes. The reference design safe shutdown earthquake (SSE) has been set to 0.3 g.

2.10. Protection of confinement structure (4.2.3.8)

Principle 175 of INSAG-3 states that "If specific and inherent features of a nuclear power plant would not prevent detrimental effects on the confinement structure in a severe accident, special protection against the effects of such accidents is provided, to the extent needed to meet the general safety objective".

As noted above (in section 2.9. and in the design description), the containment and the reactor building are designed to withstand the effects of external events such as the impacts of a crashing aircraft and a safe shutdown earthquake of 0.3 g. The containment structure is furthermore designed to withstand a double-ended break of the largest pipe - the dominant internal event with respect to pressurization of the containment vessel.

In most severe accidents (beyond Design Basis accidents) situations, the stresses and loads on the containment structure will not exceed those occurring in the design case; double-ended break of the cold leg close to the main coolant pump outlet, combined with "failure to scram" which does not make very much difference, and loss of all AC power (station blackout) for hours. Considerable margins are therefore available in the design. As noted, safety analyses have not yet identified any reasonably conceivable sequence of events that will result in a core degradation or core melt accident. Therefore, assessments of containment behaviour in the event of such accidents - or its capability to resist loads and stresses, and to confine released radioactive material, associated with them - have not been made.

In the context of present-day PWR plants, core damage situations must be taken into due account in the design, and the general intent of this key area is to address the potential for handling and retaining a molten core and the associated released radioactive material.

2.11. Monitoring of plant safety status (4.2.3.9)

INSAG principle 180 states that "Parameters to be monitored in the control room are selected, and their displays are arranged, to ensure that operators have clear and unambigous indications of the status of plant conditions important for safety, especially for the purpose of identifying and diagnosing the automatic actuation and operation of a safety system or the degradation of defence in depth."

As noted above, eg. in sections 2.2 and 2.5, the PIUS plant is provided with instrumentation and control (I&C) systems in a similar way as other PWR plants, for control and monitoring, for initiation of system functions to counteract malfunctions or deviations from proper operation, and for actuation of protective actions.

The PIUS plant I&C system may be divided up into the following main parts:

- Systems or functions needed for supervision and control of the normal operation of the plant;
- Systems or functions related to protection of plant components and systems; and
- Systems for management of the core operation.

The I&C system is predominantly based on programmable technology and equipment. The different I&C functions are performed by various types of microprocessor or computer systems. Data acquisition for process information, and the interface to process actuators, utilizes the simplest types of microprocessors, whereas the top level of the I&C system hierarchy uses powerful mini-computers, eg., for core calculations. Intermediate types of microcomputers are utilized for control and operation, logic and signal treatment.

For manual process control and for operator information, video display units (VDUs) and associated keyboards, etc. are installed in the main control room. Some equipment is also located in an auxiliary shutdown facility which can be used for shutting down the reactor and supervising its safety, if or when the control room would become unavailable.

2.12. Preservation of control capability (4.2.3.10)

Principle 183 of INSAG-3 states that "The control room is designed to remain habitable under normal operating conditions, anticipated abnormal occurrences and accidents considered in the design. Independent monitoring and the essential capability for control needed to maintain ultimate cooling, shutdown and confinement are provided remote from the main control room for circumstances in which the main control room may be uninhabitable or damaged".

As noted above (eg. in the design description and in section 2.11), an auxiliary shutdown facility is provided in the reactor building at a low location. This emergency control centre can be used for shutting down the reactor and supervising its safety, if or when the main control room would become unavailable.

2.13. Station blackout (4.2.3.11)

INSAG-3 principle 186 states that "Nuclear Plants are so designed that the simultaneous loss of normal on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage."

As noted above (in the design description and in sections 2.7 and 2.10) the PIUS thermal-hydraulic arrangement with the density locks and the surrounding reactor pool of borated water yields a high degree of insensitivity to loss of AC power; the reactor shuts down automatically when power supply to the main coolant pumps is lost; most of the heated water from the primary loop is displaced to the reactor pool, and the passive RHR system transports the heat out to the ambient air.

2.14. Control of accidents within the design (4.2.3.12)

Principle 189 of INSAG-3 states that "Provisions are made at the design stage for the control of accidents within the design basis, including the specification of information and instrumentation needed by the plant staff for following and intervening in the course of accidents".

In analysing accidents and transients in PIUS, it is assumed that any load carrying structural member may contain hidden faults that can lead to failure; simultaneous unrelated structural failures are neglected, however. Another underlying design assumption is that plant operators can make arbitrary mistakes with the plant controls at their disposal in emergency situations.

The basic safety performance can be illustrated by the plant response to a hypothetical large LOCA, a double-ended cold leg pipe rupture at a low location. Initially, there will be an outflow of primary loop water through both hot and cold leg pipe nozzles, a rapid inflow of borated water from the pool, and shutdown of the reactor. Outflowing primary loop water flashes to steam in the containment, and the containment atmosphere gas is compressed. Most of the compressed gas will be displaced to the gas compression chamber in the wetwell via the blowdown pipes and the condensation pool. The steam flowing down into this pool condenses, and the peak pressurization of the containment will be limited by the heat capacity of the pool.

The hot leg outflow stops when the water level in the vessel drops below the hot leg nozzle, and a pressure equilibrium is established between the containment and the reactor vessel. The siphon breaker arrangement (the siphon breaker proper and the parallel three other loops) provides "containment" pressure also on the inside of the cold leg nozzle; the large outflow from the reactor system stops - all by itself. The core is cooled by reactor pool water in natural circulation, and the decay heat is absorbed in the pool. The pressure in the containment attains a peak of about 270 kPa after about 1 minute, decreasing to slightly above atmospheric pressure again in about 2 hours, due to steam condensation on containment walls and structures.

The reactor pool water is cooled by the passive system arranged in four groups, each with a cooling tower on top of the reactor building. Postulating failure of one group, the reactor pool water temperature will still be kept below boiling temperature at atmospheric pressure.

This accident does not result in fuel damages, and the release of radioactive material to the containment is determined by the amount of such products present in the water prior to the accident. The iodine "spiking" will remain in the reactor water since there will be no boiling. Hence, release to the containment will be very small, and taken its moderate and short pressurization the release to the environment will be minimal; the whole body dose at the plant fence has been calculated to about 1 mrem. It may be noted that a significant reduction of requirements with respect to emergency preparedness has been a design objective for PIUS.

In addition to the deterministic analyses, and the simulations performed with thermal-hydraulic computer codes, a preliminary Level 1 PSA study has been completed in a joint effort by ABB Atom and the Italian power company ENEL SPa (formerly, the Italian State Utility). This study represents a first comprehensive review of the PIUS plant design, based on ultra-conservative assumptions. The failure frequency for the prestressed concrete vessel ended up as being somewhat higher than for a steel vessel, and a number of transients were just postulated to yield core damage even though calculations have shown that they would not. Still, the resulting "core damage" frequency is below 10^{-7}.

2.15. Mitigation and control of severe accidents

The intention behind the inclusion of this key area appears to be an ambition to open up a discussion of ways and means to cope with a core melt situation; i.e., to address whether or not the releases of radioactive material to the environment can be controlled in a reliable way.

As noted above (in the design description and in sections 2.2, 2.3, 2.8 and 2.10), analyses performed by ABB Atom and by Los Alamos National Lab. in the US have not yet identified any (realistically) conceivable accident sequence that will result in core damage. Hence, assessments of possible consequences of such hypothetical situations have not been given any priority in the design activities. With limited manpower resources, such assessments represent a waste of time and money.

3. LIST OF MAIN PARAMETERS

1. Station output

Rated thermal power of reactor	2 000 MW
Net rated plant output at	640 MWe
A cooling water temperature of	15°C

2. Fuel assembly

Array	18 x 18
Number of fuel rods	312
Number of guide tubes for absorber/	0*)
in-core instrumentation	4
Full length (without control spider)	2.82 m
Fuel rod, length	2.625 m
- outside diameter	9.5 mm
- cladding material	Zircaloy 4
Fuel pellet, length	10 mm
- diameter	8.2 mm
- nominal diametrical clearance	0.16 mm
- material	UO_2*)
- density	10.4 10^3kg/m^3

3. Reactor core

Number of fuel assemblies	213
Active height	2.50 m
Equivalent diameter	3.75 m
Rod cluster control assemblies absorber	NA
Number of assemblies	
Absorber rods per assembly	
Enrichments, first core (average)	2.0%
reload	3.5%
(H_2O/UO_2) volume ratio	≈1.8
Average fuel burnup (equilibrium core)	45 500 kWd/kgU
Total weight of U	80.5 10^3 kgs
Heat transfer surface in core	5 000 m^2
Mean linear heat rate of fuel	11.9 kW/m
Mean power density in fuel	24.8 kW/kgU

4. Reactor Coolant System

Design conditions:	
- pressure	10.5 MPa
- temperature	315°C

*) *In fresh fuel assemblies, up to 16 fuel rods will contain burnable absorber material in addition to fuel*

Operating conditions:	
- pressure at vessel inlet	9.50 MPa
- pressure at vessel outlet	9.30 MPa
- temperature at vessel inlet	260°C
- temperature at vessel outlet	289.3°C
Nominal flow rate	13 200 kg/s[**)]

5. <u>Reactor vessel</u>

A. Prestressed Concrete Reactor Vessel (PCRV)

Overall height (without the vessel upper part)	44 m
Overall width	26.8 x 26.8 m
Inside diameter (max cavity diameter)	12.2 m
Cavity volume (to top of concrete)	3 300 m^3
Net reactor pool water volume (above top of core)	2 300 m^3
Wall thickness (minimum)	7.4 m
Stainless steel liner thickness	15 mm
Total weight (without water)	63 000 10^3kgs
Design pressure	10.5 MPa
Design temperature	95°C

B. Pressure Vessel Upper Part (PVUP)

Overall height with the head	14.4 m
Overall width	9 m
Inside diameter	6.1 m
Wall thickness (minimum)	0.18 m
Minimum stainless steel cladding thickness	10 mm
Inlet/outlet nozzle inside diameter	635/665 mm
Mass (including head)	550 10^3kgs
Material (forged rings)	pressure vessel steel, SA 533 B
Design pressure	10.5 MPa
Design temperature	315°C
Neutron fluence for service life	NA n/m^2

6. <u>Reactor coolant pump</u>

Type	Variable speed, wet asynchronous motor & gland-less shaft pump
Number	4
Design conditions:	
- pressure	10.5 MPa
- temperature	315°C

[**)] *In PIUS, the coolant circulation through the core and up the riser always takes place in a natural circulation mode; forced circulation applies only to the water transport from the top of the riser and back to the core inlet plenum, via the steam generators.*

Design flow rate (at 100% reactor power)	3300 kg/s
Pump casing material	SA 533, Class 2, Grade B
Speed (at 100% reactor power)	1450 rpm
Power at pump shaft (at 100% reactor power)	2 500 kW
Weight	27 10^3kgs
Coast-down time	≈12 s
Pump motor inertia	75 kgm^2

7. Steam generator

Type	Vertical straight once-through
Number	4
Heat transfer surface	24 000 m^2
Number of heat exchanger tubes	8 000
Tube dimensions	14.2/15.9 mm
Tube length	15 m
Outside diameter of shell	2.5 m
Total height	19 m
Transport weight (SG proper)	103 10^3kgs
Total installed weight, incl. Reactor coolant pump	130 10^3kgs
Shell material	SA 533, Class 2, Grade B
Tube sheet material	SA 508, Class 3a
Tube material	Inconel 600
Steam pressure at SG outlet	4.0 MPa
Steam temperature	270 C
Steam output	253 kg/s
Feedwater temperature	210 C
Water volume of secondary side***)	8.4 m^3
Steam moisture at outlet from SG****)	0%

8. Pressurizer

Total volume	150 m^3
Steam volume	100 m^3
Design pressure	10.5 MPa
Design temperature	315°C
Heating power of the heaters, each (In PIUS, the heaters are located in a "boiler" external to the reactor pressure vessel)	350 kW
Number of heaters	8
Inside diameter*****)	6.1 m
Total height	NA
Material	NA
Transport weight	NA

***) about 50 % is water in two-phase mixture

****) steam is superheated

*****) In PIUS, the pressurizer is integrated into the PVUP; its inside coincides with the PVUP wall

9. Containment

Configuration	Primary and secondary
Material	Reinforced concrete with steel liner
Gross volume	90 000m^3
Net volumes (drywell/wetwell/cond. pool)	20 000/20 000/2 000 m^3
Design pressure	0.5 MPa
Overall inside height	61 m
Overall width	63 m
Design leak rate (for calculation of releases)	1.0%
System of corium retention	NA

REFERENCES

[1] U. Bredolt, J. Fredell, K. Hannerz, J. Kemppainen, T. Pedersen, C. Pind; "PIUS - The Next Generation Water Reactor", Proc Int Top Mtng on Safety of Next Generation Power Reactors, Seattle, WA, May 1-5, 1988, pp 476-487

[2] K. Hannerz, L. Nilsson, T. Pedersen, C. Pind; "The PIUS PWR, Aspects of Plant Operation and Availability", Nucl Techn, Vol. 91, No. 1 (July 1990), pp 81-88.

[3] D. Babala, U. Bredolt, J. Kemppainen; "A Study of The Dynamics of SECURE Reactors; Comparison of Experiments and Computations", Nucl Eng. & Des. 122 (1990), pp 387-399

[4] T. Pedersen; "Reactors take a large step towards "inherent safety"", Power Generation Technology, 1990/91, pp 131-135

[5] T. Pedersen; "PIUS - Status and perspectives", Nucl. Eng. & Des. 136, (1992), pp 167-177

[6] K. Hannerz, T. Pedersen; "PIUS - the nuclear reactor of tomorrow", ABB Review No 2, 1990, pp 3-14

[7] J. Fredell, C. Pind; "Summary of theoretical analyses and experimental verification of the PIUS density lock development program", IAEA-TECDOC-677, Progress in development and design aspects of advanced water cooled reactors (A TCM in Rome, Sept 1991), pp 213-219

[8] T. Pedersen; "PIUS - A New Generation of Nuclear Power Plants", Proc. ASME/JSME Nuclear Engineering Conference (ICONE-2), San Francisco, CA, March 1993 - Volume 2, ASME 1993, pp 627-631

Next page(s) left blank

Appendix I
DESIGN INFORMATION ON SOME OTHER PLANTS
(for reference)

BASIC INFORMATION ON DESIGN FEATURES OF THE AC-600 ADVANCED REACTOR PLANT

Min Yuan-You, Zhang Shen-Ru, Zhang Yi-Ming
Lu Lian-Hong, Xu Chang-Rong
China National Nuclear Corporation CNNC,
Beijing, China

1. BRIEF DESCRIPTION OF THE CONCEPT

1.1. The main elements of the safety philosophy

The AC-600 design based on Qinshan phase II standard PWR nuclear power plant (2 x 600 MWe) is expected to improve the economy and safety of the nuclear power plant through use of system simplification, passive safety, and modular construction. The AC-600 will become a major type of reactor for the next generation of 600 MWe nuclear power plants in China. The AC-600 has a large safety margin of operation because of the small power density of the reactor core. The high natural circulation cooling ability due to a small flow resistance of the primary system loop is very useful for reactor core decay heat removal during accidents. The AC-600 has a large reactor pressure vessel, a large pressurizer and a large water volume in the primary systems so as to function as accident mitigation. The AC-600 design, eliminating the high head safety injection pumps, utilizes full pressure core makeup tanks and larger accumulators for the engineered safety features. The passive containment cooling system is used as the ultimate heat sink. All of those measures mentioned above increase both the reliability and the capacity of the engineered safety very much, largely improving the safety of AC-600. The major design targets of AC-600 are given in Table 1.

Table 1: Major Design Targets for AC-600

Parameter	Design Target
Construction cost	about 20% less than that of Qinshan Phase II NPP
Core melt frequency	1 x 10^{-5} to 1.5 x 10^{-6}/r-y
Availability factor	> 85%
Refuelling period	18 months
Construction period	5 to 6 years
Plant life time	60 years
Plant personnel exposure dose	50-100 man-rem/year

The safety goals of nuclear power plants should include not only the protection of the environment and the public, but also the protection of the plants themselves as well. The two sides of the safety goals can not be separated completely but are closely related to each other. It is quite evident that only under the prerequisite of the safety of the nuclear power plants themselves the goals of the environment safety and the public health can really be achieved. Increasing the plant's own safety and preventing core melt should be emphasized so as to restore the public confidence in nuclear power.

The average linear power density of the AC-600 fuel rod is 137.8 W/cm, much smaller than that of Qinshan phase II (160.87 W/cm). The small core power density makes for the reactor to have large thermal safety margins for normal operation and accident conditions.

The AC-600 design uses Gd_2O_3 burnable poison to reduce the excess reactivity of the reactor and the critical boron concentration. Because of the small critical boron concentration, a large negative temperature coefficient of reactivity can be obtained. The small excess reactivity and the large negative temperature coefficient of the core is one of the AC-600 design characteristics, largely improving the passive and inherent safety of the reactor to prevent power excursions induced by reactivity accidents.

The measures of elevating the vertical distance between the steam generators and the reactor core, and reducing the flow resistance, are used in the AC-600 design to increase the natural circulation cooling flow rate of the primary coolant. If the reactor operates at 25% of the rated power, the natural circulation flow is 4852 t/h (15.12% of the rated flow rate) after the reactor coolant pumps shut down. The natural circulation flow rate increase is a very important part of the passive safety of AC-600.

The passive emergency residual heat removal system on the secondary circuit side is mainly used in the events of station blackout, main steam line rupture or loss of feedwater. The system consists of an emergency feedwater tank, an emergency air cooler, valves and pipes for each loop. When station blackout occurs, the decay heat generated in the reactor core can be removed through use of natural circulation flow in the primary coolant system, in the secondary coolant system, and to the atmosphere, respectively.

In order to increase the reliability of the safety injection system, two full pressure core makeup tanks, two accumulators and four low head safety injection/recirculation pumps, which are installed in the containment sumps, are utilized in the AC-600 design. In case of a large LOCA, the flow rate into the RCS from a core makeup tank is larger than that from a high head safety injection pump in the conventional design. It is necessary for the AC-600 to use active pumps which can perform the functions of the low head safety injection/recirculation system.

The passive containment cooling system is used to remove the heat from the inside to the outside of the containment during a LOCA or a main steam line rupture inside the containment. First, the water in the tank on the top of the containment will be sprayed out to the surface of the steel shell of the containment by gravity, cooling the shell so as to decrease the pressure and the temperature. After the tank on the top of the containment becomes empty, the natural circulation flow of air through the annulus between the steel shell and the concrete shell can remove the heat from the inside to the outside of the containment continuously. At the same time, the low head safety injection/recirculation pumps which are installed in the containment sumps can withdraw the borated water from the sumps into the reactor coolant system. The water absorbs the core decay heat and flows out through the break point (in LOCA condition).

1.2. Description of the reactor plant

1.2.1. General characteristics

The AC-600 reactor plant is based on Qinshan phase II (2 x 600 MWe PWR NPP). But it is improved and enhanced on the basis of Qinshan phase II (QS-II).

The primary circuit of the AC-600 uses 2 loops connected in parallel and symmetrically to the reactor, a pressurizer, and a relief tank. The flow scheme and drawing of the reactor building are shown in Fig. 1 and 2. Nomenclature, list and quantity of the main components shown in Fig. 1, are given in Table 2.

1.2.2. Reactor

A schematic drawing of the reactor pressure vessel is shown in Fig. 3. The reactor core consists of 145 17 x 17 advanced fuel assemblies, 17 control rod assemblies and other fuel associated assemblies. There are 45 black rod (Ag-In-Gd) and 12 grey rod (stainless steel) assemblies in the core. The burnable poison (Gd_2O_3) is solid-melted in the fuel. The average burnup is 42000 MWd/tU. The reactor vessel encloses all components of the reactor core. It is made of SC 508-3 steel made in China. Because of the lower power density in the core and the larger vessel inside diameter, it is much safer during the 60 years design life of the plant. The nozzles of the control rod drive mechanism (CRDM) and the in-core instrumentation are located on the closure head. There are no penetrations in the reactor pressure vessel below the level of the reactor coolant nozzles.

The pressurizer is the same as for the Qinshan phase II. Its total volume is 36 m^3. The CRDM for QS-II will be adopted in the design for the AC-600, except that the wires to be used in the electromagnetic coils for the AC-600 CRDM are melting-extruded. The operating temperature of the coils will be more than 300°C (about 350°C).

1.2.3. Reactor coolant pump, steam generator and pressurizer

The reactor coolant pump (RCP is of the mixed flow, canned motor pump type. There are four canned pumps connected to the steam generator bottom heads directly. Lubrication and cooling of the RCP are performed with water. To increase the rotating inertia of the canned motor pump, a motor and pump design with a rotating inertia of 0.15 t-m^2 will be employed.

The steam generator is of the vertical U-tube type used in Qinshan phase II. The material of the U-tubes is Inconel-690. Two canned pumps are welded reversely on the steam generator bottom head. In this case, the U shape cross-over leg of the coolant pipe is eliminated.

1.2.4. Emergency core cooling system

The AC-600 utilizes an emergency core cooling system that is based on the principle of combining of passive and active features. There are 3 subsystems for the emergency core cooling system.

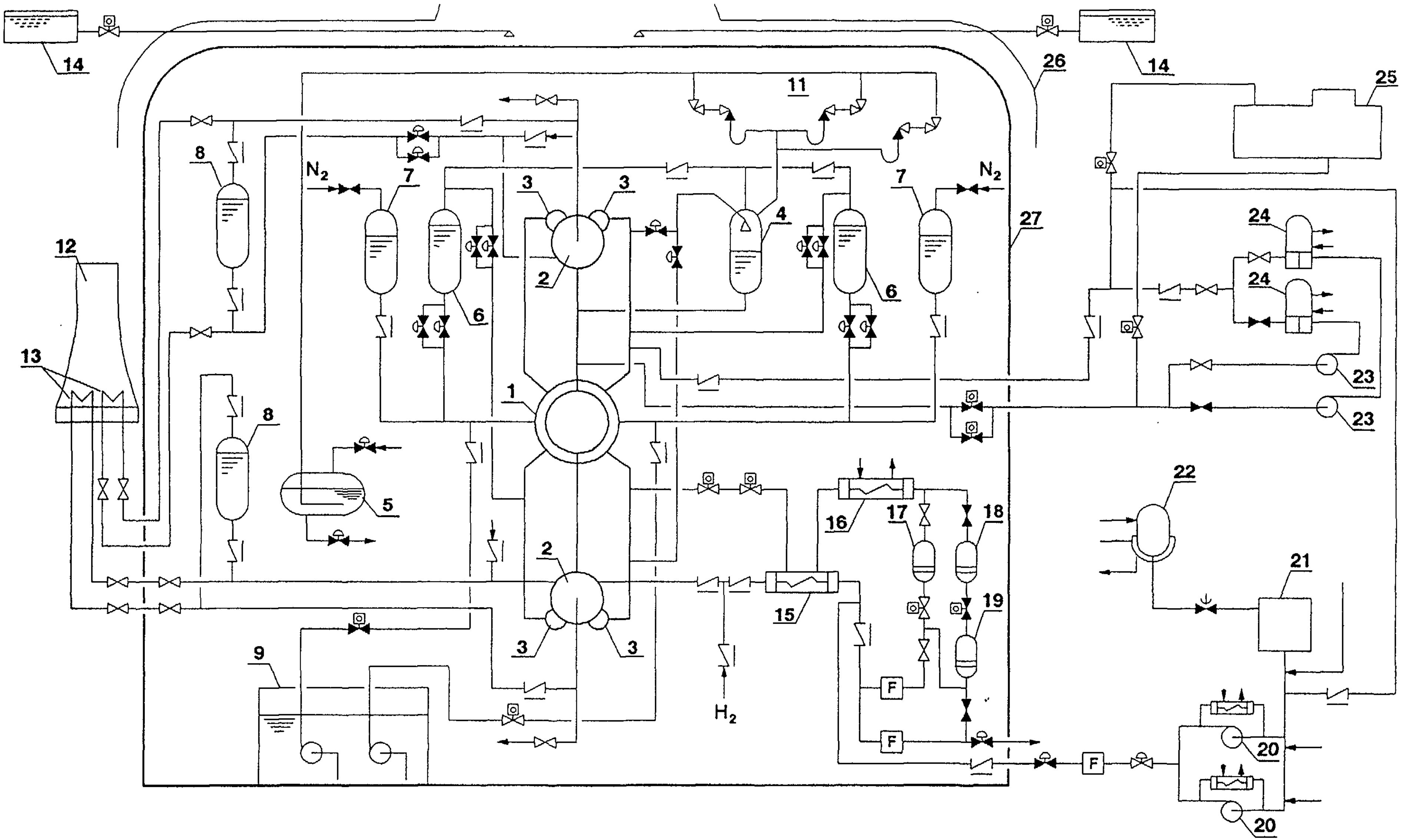


Fig. 1: AC-600 nuclear island

Table 2: (corresponding to Fig. 1).

Nr.	NAME	QUANTITY
1	reactor	1
2	steam generator	2
3	primary coolant pump	4
4	pressurizer	1
5	relief tank	1
6	core makeup tank	2
7	accumulator	2
8	emergency water tank	2
9	special sump	2
10	low pressure safety injection pump	4
11	safety valve	3
12	chimney	1 or 2
13	emergency air cooler	2
14	water storage tank	1
15	regenerative heat exchanger	1
16	letdown heat exchanger	1
17	mixed bed exchanger	1
18	mixed bed exchanger	1
19	cation bed exchanger	1
20	makeup water pump	2
21	boric acid storage tank	1
22	boric acid makeup tank	1
23	spent fuel pit cooling pump	2
24	spent fuel pit heat exchanger	2
25	spent fuel pit	1
26	protective shell	1
27	containment (steel)	1

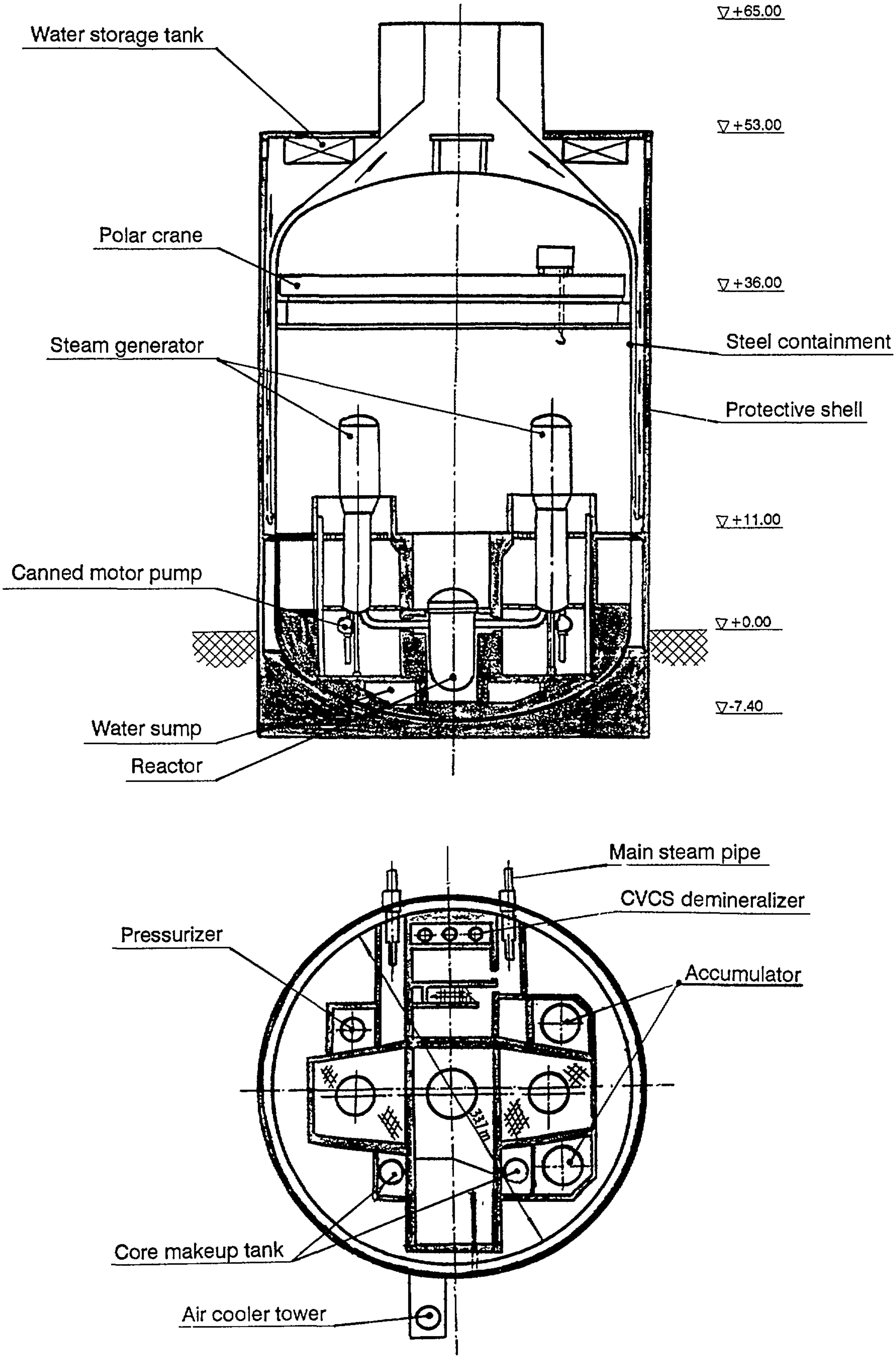


Fig. 2: Reactor building plane arrangement

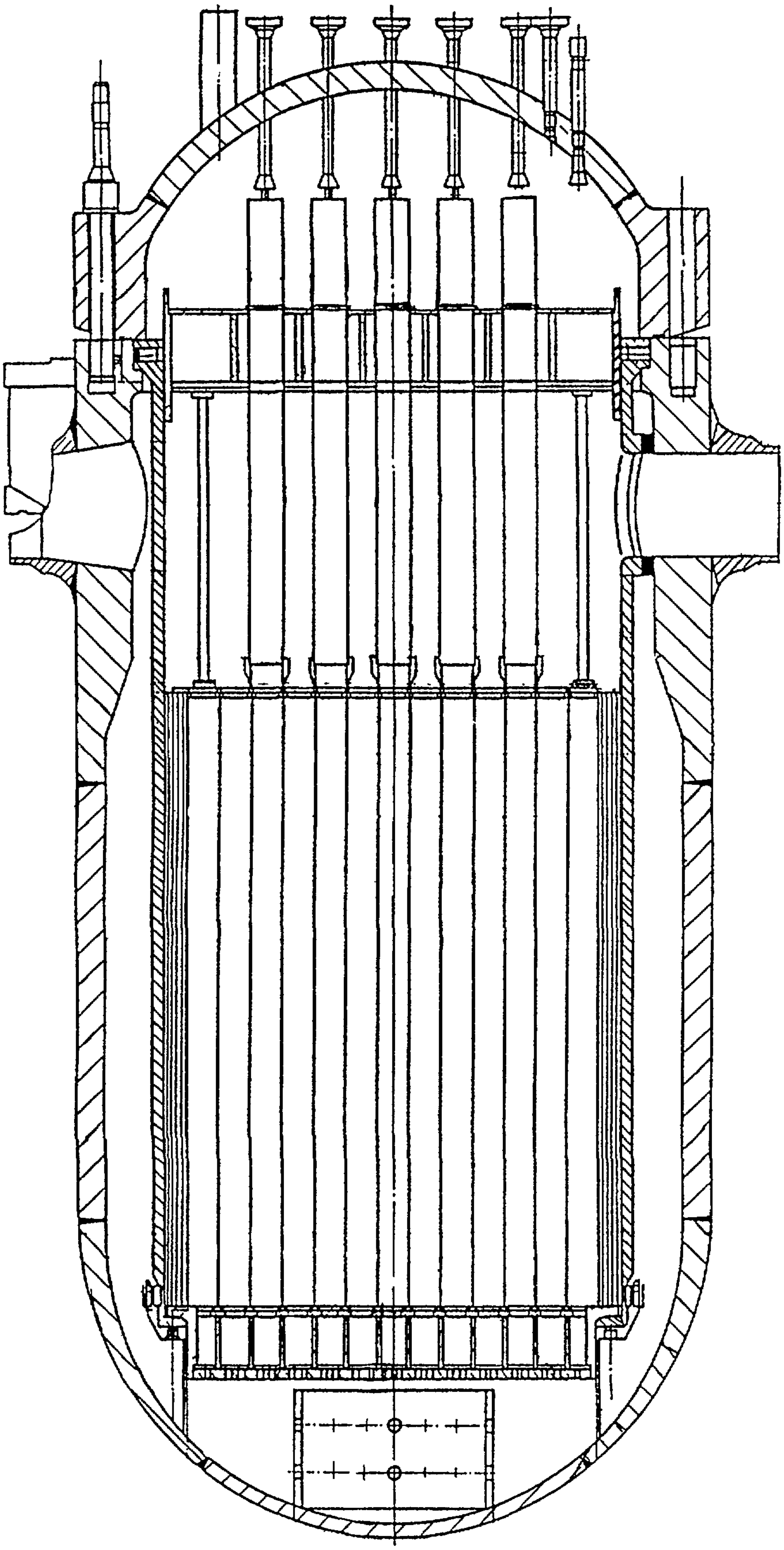


Fig. 3: Reactor vessel and internals

The high pressure injection subsystem consists of 2 reactor core makeup tanks. The middle pressure injection subsystem consists of 2 accumulators. The low pressure injection and long term cooling subsystem consists of 4 low pressure injection pumps taking suction from 2 special sumps in the containment. The low pressure injection pump is of the vertical phreatic water type. The main functions of the emergency core cooling system are as follows:

- To supply water to the reactor in the event of abnormal leakage.
- In the event of LOCA, to inject water into the reactor core and provide long term core cooling.

1.2.5. Passive residual heat removal system

The function of this system is to remove the reactor core residual heat when the reactor loses its normal cooling resulting from station blackout or other accidents.

This system has two trains. Each train consists of an emergency water tank and an emergency air cooler. When blackout or other accidents occur, the isolation valves located at the outlet pipe of the emergency water tank are opened by a low-low water level signal for the steam generator, so that the emergency water tanks provide water to the secondary side of the steam generator by gravity and maintain the water level. The water in the steam generator absorbs the heat from the reactor coolant, when the water is heated into steam. The steam rises and passes through the emergency air cooler where the steam is condensed into water. Simultaneously, the heat is transferred to the atmosphere. The condensed water returns to the steam generators by gravity, thereby a continuous natural circulation path will be established. Because of the cooling of the secondary side of steam generators, the corresponding natural circulation in the reactor coolant system will also be established. In this way, the residual heat of the reactor core will be transferred to the atmosphere.

1.3. List of the accident analysis

The following accidents will be analyzed in the AC-600 design in order to provide some important parameters for AC-600 engineered safety systems design and safety assessment.

1.3.1. Increase of heat removal by the secondary system

- Reduction of feedwater temperature caused by feedwater system malfunctions
- Increase of feedwater flow rate caused by feedwater system malfunctions
- Excessive increase of secondary steam flow rate
- Accidental main steam depressurization
- Main steam line rupture

1.3.2. Decrease of heat removal by the secondary system

- Reduction of steam flow rate cause by steam pressure regulator failure
- Loss of external load
- Turbine trip
- Inadvertent closure of main steam isolation valves

- Loss of condenser vacuum
- Loss of non-emergency AC power to the plant auxiliaries
- Loss of normal feedwater flow
- Feedwater system pipe break

1.3.3. Decrease of reactor coolant system flow rate

- Partial loss of forced reactor coolant flow
- Complete loss of forced reactor coolant flow
- Reactor coolant pump shaft seizure
- Reactor coolant pump shaft break

1.3.4. Reactivity and power distribution anomalies

- Uncontrolled rod cluster control assembly bank withdrawal from a subcritical or low power start-up condition
- Uncontrolled rod cluster control assembly bank withdrawal at power
- Rod cluster control assembly misalignment
- Inadvertent drop of rod cluster control assembly
- Boron dilution accident caused by chemical and volume control system malfunction
- Rod cluster control assembly ejection

1.3.5. Increase in reactor coolant inventory

- Inadvertent operation of safety injection system during power operation
- Chemical and volume control system malfunction that increase reactor control coolant inventory

1.3.6. Decrease in reactor coolant inventory

- Inadvertent opening of a pressurizer pilot operated safety valve
- Failure of small lines carrying primary coolant outside containment
- Steam generator tube rupture
- Small break LOCA
- Intermediate break LOCA
- Large break LOCA

1.3.7 Radioactive release from a system or component

- Waste gas system failure
- Waste liquid system failure
- Fuel handling accident
- Spent fuel cask drop accident

1.3.8. Anticipated transients without scram

- Loss of normal feedwater supply
- Loss of offsite power

1.4. List of beyond design basis accidents (severe accidents)

- Total loss of ultimate heat sink
- Loss of main and auxiliary feedwater
- Station blackout
- Loss of containment spray pumps of safety injection pumps

2. DESCRIPTION OF 15 SPECIFIC DESIGN AREAS AS SELECTED FROM INSAG-3

In the following sections the reference to INSAG-3 is put in parentheses after each heading.

2.1 Plant process control systems (4.2.2.1.)

Plant process control systems fulfil the automatic control of the following main controlled parameters:

- neutron flux in the core
- primary pressure
- secondary pressure
- water level in the steam generators
- water level in the pressurizer

The design value of the reactor neutron flux is maintained with the control bank of neutron absorbers, consisting of several rod cluster control assemblies, within ± 2% of its nominal value.

The design value of the primary pressure is maintained by the pressurizer electric heaters and by spray valves on the pressurizer spray line from the reactor coolant pump exit side to the steam phase of the pressurizer within ± 0.3 MPa.

The design value of the secondary pressure is maintained by an appropriate balance of reactor power and steam flow from the steam generators to the turbine or to the steam dumping devices within ± 0.2 MPa.

The design value of the water level in the steam generators is maintained with the help of the steam generator feed water supply controller actuating the control valve on the steam generator feed water line within ± 180 mm of its nominal level.

The design value of the water level in the pressurizer is provided by the level controller, actuating the control valves located on the make-up line, and make-up pumps, to keep within normal value.

2.2. Automatic safety systems (4.2.2.2.)

2.2.1. List of automatic safety systems:

- reactor emergency protection system
- primary overpressure protection system
- emergency core cooling system
- system of passive residual heat removal from the secondary side of the steam generator
- passive cooling system from the containment
- system of quick-acting isolation valves in the main steamlines
- secondary overpressure protection system
- diesel-generator system
- system of reliable direct current power supply

2.2.2. Reactor emergency protection system

The reactor emergency protection system provides reliable switch-off of the electric power supply to the rod drive, causing the emergency shutdown rods to drop into the core. In this case, the disappearance of the signal of the original cause does not stop the initial action of the emergency protection (for more detail, see section 2.5).

2.2.3. Primary circuit overpressure protection system

The system comprises three identical pilot safety valve assemblies, which discharge steam or steam-water mixture from the steam phase of the pressurizer to the relief tank when the pressure in the pressurizer increases above the permissible one. The subsystem for receiving the steam or steam-water mixture involves a relief tank and pipelines connecting it with the outlets of the safety valves.

2.2.4. Emergency core cooling system

The emergency core cooling system (ECCS) comprises the following complex of subsystems initiated automatically:

- subsystem of core make-up tank with full pressure (high pressure safety injection subsystem)
- subsystem of accumulator with nitrogen under pressure
- subsystem of low pressure active safety injection and recirculation

For fulfillment of ECCS functions, except the subsystems of low pressure active safety injection and recirculation, sources of alternating current are not required. The air-operated valves, needed for the function of emergency heat removal, are driven by compressed air from the compressed air storage tanks. The power supply of the subsystems of low pressure active safety injection and recirculation are provided by the diesel generators or by the offsite power source (during the recirculation stage after LOCA).

2.2.5. System of passive residual heat removal from the secondary side of the S.G.

The passive residual heat removal system removes the residual reactor power during a plant blackout with the aid of natural circulation on the secondary side of the S.G. It consists of two independent trains, each of them being connected via the S.G. to the respective reactor loop. Each train has an emergency feedwater tank, a heat exchanger cooled by air and located outside of the containment, and piping for steam and condensate circulation. The fail-open valves on the piping are driven by compressed air. The air-cooled heat exchanger rejects decay heat via the steam generators into the atmosphere outside the containment.

2.2.6. Passive cooling system from the containment

The passive containment cooling system removes heat from the containment in accidents caused by LOCA of the primary circuit. Steam released is condensed on the inside of the containment shell and cooled on the outside natural circulation air and gravity drain of water from the elevated tanks above the containment. The heat released to inside of the containment is rejected to the atmosphere from the containment. The pressure of the atmosphere inside the containment is kept below the permissible design value.

2.2.7. System of quick-acting isolation valves in steamlines

The quick-acting isolation valves in steam lines causes close at:

- level in steam generators increase above the permissible one
- increase of radioactivity in steam generators above the permissible one
- reception of signals of a steamline rupture

The system provides for

- protection of the turbine from steam of high humidity
- prevention of radioactivity release from steam generators
- restriction of steam blowdown during rupture of the secondary circuit

2.2.8. Secondary circuit overpressure protection system

This system prevents the secondary circuit pressure to increase above the permissible level of 110% of secondary design pressure. It incorporates a power operated relief valve and seven safety valves. These valves reject steam into the atmosphere.

2.2.9. Diesel generator system

Two physically separated diesel generators provide power supply to the safety related systems, involving the recirculation pumps of the subsystem of low pressure active recirculation.

2.2.10. System of reliable direct current power supply

This system consists of storage batteries. It provides the power supply to electromagnetic circuits for operating of safety systems and for recording of necessary post-accident parameters.

2.3. Protection against reactivity transients (4.2.3.1)

During normal operation , the reactor's neutron power and the process parameters are maintained automatically by the reactor control system. Protection against transients due to the introduction of reactivity is assured by the reactor protection system. When reaching the setpoints of neutron flux or reactor period, the reactor protection system will warn the operators to take actions or will trip the reactor so that reactor safety can be ensured.

2.4. Reactor core integrity (4.2.3.2.)

2.4.1. Permissible limits of fuel cladding damage

2.4.1.1. Normal operating limits

- Number of fuel rods with gas leaktightness flaws, and with direct contact of nuclear fuel with coolant, are 0.1% and 0.01% respectively.
- 7.4 x 10^{10}Bq/t of iodine nuclide radioactivity in the primary coolant should not be exceeded, and iodine nuclide radioactivity in the steam generator secondary water should not exceed 10^4Bq/t.

2.4.1.2. Fuel cladding limits for condition 4 events

- Calculated maximum cladding temperature shall not exceed 1204°C.
- Maximum cladding oxidation shall nowhere exceed 0.17 times the total cladding thickness.
- The total calculated amount of hydrogen produced by the chemical reaction of the cladding with water or steam shall not exceed 0.01 times the hypothetical amount which would be produced if all the cladding material enclosing the fuel (excluding the plenum cladding) reacted.
- Calculated core geometry changes shall be such that core long-term cooling is maintained, and that safety shut-down is performed.

2.4.1.3. Effects of fuel cladding damage

- Not leading to a considerable amount of radioactivity release from fuel rods
- Not leading to a considerable steam-Zirconium reaction extent
- No fuel material escape out of the cladding impairing core cooling; nor affecting post-accident core disassembly.

2.4.2. Under design condition the following is ensured:

- Retention of the required geometry and position of fuel rods in the fuel assembly and of the fuel assemblies in the core.
- Necessary margin of axial or radial expansion of fuel rods, taking into account the variation of geometry as a result of temperature and radiation effects, pressure differences, interaction between fuel pellets and fuel rod cladding.
- The core structure to be able to withstand all mechanical loads.
- Fuel rods and assemblies to be able to withstand coolant caused effects such as vibration, pressure drop, pressure pulsation and flow instabilities.

- Normal movement of control assemblies and emergency shut-down are ensured.

2.4.3. Design features of the fuel assembly

- square array lattice of fuel assembly, 17 x 17-25 AFA modified type
- burnup depth 50000 MWd/tU

2.4.4. Monitoring of reactor core integrity

- post-accident in-reactor level monitoring
- in-reactor loose and vibratory part monitoring

2.5. Automatic shutdown systems (4.2.3.3.)

When any accidents occur, the reactor protection system is designed to perform reactor trip.

The emergency protection is actuated by de-energizing the control rod drive mechanism. The following parameters are used to execute the reactor protection system:

- increase of neutron flux
- decrease of reactor period
- OTΔT and OPΔT
- decrease of pressure in the reactor
- increase of pressure in the reactor
- decrease of the flow rate in the reactor
- decrease of water level in SG
- increase of water level in SG
- decrease of the reactor coolant pump speed
- signal of safety injection

The reactor protection system trips the reactor, meeting the design criteria under all design conditions.

To mitigate the consequences of ATWS, the protection actions will be taken to trip the turbine and to start the auxiliary feed water system.

2.6. Normal residual heat removal (4.2.3.4.)

In the first stage of normal plant shutdown, the residual heat of the reactor and the coolant system is transferred to the secondary loop through the steam generators. The steam then generated enters the condenser freezer through the turbine bypass system to be condensed. The auxiliary feedwater system supplies the steam generator with water. The whole process goes on till the pressure of the coolant system drops to 2.8 MPa and the temperature to 180°C.

In the second stage of shutdown, residual heat removal is accomplished by the residual heat removal system. The residual heat removal system and spent the fuel pool cooling and purification system share the same equipment. It consists of two independent series, each of which includes one pump and heat exchanger cooled by equipment coolant. During normal plant operation, this system acts as the spent fuel pool cooling and purification system. During plant shutdown, one series of it is used to transfer reactor residual heat. At the same time the spent fuel pool is also cooled till the coolant pressure is under 0.1MPa. Coolant temperature drops and will be kept at cold shutdown temperature.

During plant shutdown and cooling process, the coolant pump is always in operation. It does not stop until coolant temperature drops to 70°C. Before it stops totally, coolant circulates in coolant loop. After that, coolant is driven by the spent fuel pit cooling pump.

2.7. Emergency residual heat removal (4.2.3.5.)

Under the condition of a big leakage from the reactor coolant pressure boundary, emergency residual heat is removed by the emergency core cooling system and the passive containment cooling system. The water volume of the primary system is guaranteed by the emergency core coolant system in order to keep the fuel assemblies in the pressure vessel covered with water.

Under the condition of completely intact pressure boundary, the typical situation in which emergency residual heat removal is required is blackout. At this time, the passive heat removal system on the secondary side of the steam generators is automatically put into operation. Through natural circulation of primary coolant, natural circulation of secondary loop steam and condensed water, and natural convection of air in special ducts outside the containment, residual heat is removed to atmosphere. By this system the coolant temperature and pressure can be brought to the corresponding values for cold shutdown, or till the power is back on. Besides the condensed water from the air cooled heat exchanger, secondary side system feed water is also available from the emergency feedwater tank. So the water volume is kept at the required value by natural circulation in the secondary system. See Section 2.2. for a more detailed presentation.

2.8. Reactor coolant system integrity (4.2.3.6.)

2.8.1. General

The integrity of the reactor coolant pressure boundary is provided by appropriate design and provisions, such as in-service inspection, monitoring, test and quality control, etc. Since the operating pressure and the temperature in the primary loops are limited, the integrity of reactor coolant system is further ensured. The materials for all components are subject to exact choice and are compatible with the coolant. All components of the reactor coolant system are subject to calculations regarding strength, stress and strain under design and design basis accident conditions. Seismic analyses are also performed. The leak detection before break is also used in the system design.

2.8.2. Overpressure protection of the reactor system

The reactor coolant systems are equipped with overpressure protection. The systems are designed in compliance with RCC-P "Design and construction rules for France 900 MWe PWR plant". The system overpressure is not exceeded under normal transients and design basis accident conditions.

2.8.3. Inspection and tests of reactor coolant pressure boundaries

Inspection and tests of the reactor coolant pressure boundaries are performed in compliance with the in-service inspection program and are considered during design. Contents of the inspection and tests mainly include:

- Hydraulic test of system components is completed before components are moved out of manufacturing plant.
- Preparatory tests are performed before plant operation under cold and hot conditions.
- In-service inspection for welded joints and overlays are provided during plant operation.
- Periodical inspections of the reactor pressure vessel inside surfaces and the reactor internals are performed during the design life.
- Non-periodical extraordinary tests are performed after an operating earthquake or after serious accidents.
- The necessary accessibility and working space are considered during plant design.

2.8.4. Detection of leaks from reactor coolant systems

- Coolant leakage across steam generator tubes or tube sheets into secondary circuit is performed by reference isotopes I^{131} , I^{135}, Na^{24}, $K^{42.}$
- Coolant leakage of reactor coolant pressure boundary into the reactor containment, is performed by sump level and/or sump flow monitoring.

2.8.5. Concept of ensurance of reactor vessel integrity

All materials used or the manufacture of the vessel are qualified and demonstrated by long-time operational experience (QS-I, QS-II or other reactors).

All parts of the reactor pressure vessel use forgings and are assembled by welding between the parts.

The upper head is removable; the connection between upper head and lower body is done by employing a flange and gaskets. There are no weldings in the core zone.

The reactor pressure vessel is subject to non-destructive tests, hydraulic tests and quality control during manufacturing in the factory, subject to pre-operational tests before operation and subject to periodic in-service examinations during plant operation.

All welded joints and inner cladding shall be subject to non-destructive tests. Destructive tests are performed by surveillance specimens of vessel materials.

2.8.6. Materials of the reactor coolant pressure boundaries

All components of the reactor coolant pressure boundaries are made of common materials demonstrated internationally. Base materials of the reactor pressure vessel, the steam generator and the pressurizer are low-alloyed carbon steel which is made in China. The cladding of its internal surface are all austenitic stainless steel. Various properties are ensured, such as the mechanical properties, good weldability and resistance performances to the effects of irradiation, etc.

2.9. Confinement of radioactive material (4.2.3.7.)

2.9.1. Confinement of radioactive material during normal condition and operational occurrences is provided by maintaining the integrity of all barriers: fuel rod claddings, primary pressure boundary and steel containment.

2.9.2. Confinement of radioactive materials released from the primary circuit in design basis accidents is provided by maintaining steel containment integrity.

2.9.3. Control of radioactive materials in design basis accidents with a leak from primary to the secondary circuit is provided by isolation of the steam generators on the steam and water side with the help of quick-acting shut off valves, actuated by a signal of radioactivity increase in the damaged steam generator.

2.9.4. Confinement of radioactive materials released from the fuel and the primary circuit in beyond-design accidents is provided by the steel containment and by operation, if necessary, of the filtration plant for controlled removal of the atmosphere inside the containment.

2.10. Protection of confinement structure (4.2.3.8.)

2.10.1. Loads acting upon the protective shell of the steel containment

Seismic effects

The design is performed taking into account of two levels of seismicity: an operation basis earthquake (OBE) of magnitude 7 on the MSK-64 scale and a safety shutdown earthquake (SSE) of magnitude 8 on the MSK-64 scale.

The reactor plant equipment is calculated for seismic effects. During the operating basis earthquake, normal operation of the reactor plant is provided. During the safety shutdown earthquake rector, a safe plant shutdown and cooling is provided. All civil structures, process components and equipment, pipelines, instrumentations, and so on, depending upon the degree of their responsibility for safety ensurance during seismic effects and availability after an earthquake, are divided into 3 seismic categories. Components and systems of category 1 shall fulfill their safety functions during and after an earthquake of SSE intensity. After an OBE availability is maintained.

The seismic category includes:

- Systems for normal operation, failure of which during an SSE may results in radioactivity releases causing excessive population doses in comparison with the specified values for SSE condition.
- Safety systems for keeping the reactor in a subcritical state, for emergency heat removal and for confinement of radioactive products.
- Structures and equipment which could impair above functions as a consequence of an SSE.

The design considers the possibility of using a special seismic isolator located under the base plate.

Loads due to wind, hurricane and tornado

The wind external load for the first category buildings and constructions is assumed to have a hurricane wind speed of 25 m/s. Effects of tornado for the first category building and construction are taken into account in the design with the following characteristics and physical parameters:

- Maximum horizontal speed of rotation of tornado wall: 85 m/s.
- Translational motion speed of tornado: 22 m/s.
- Tornado radius: 45 m.
- Differential pressure between centre and periphery of the whirlwind: 8.5 kPa.
- Impact of missiles carried away by a whirlwind with a speed of 26 m/s.

External explosion and airplane crash

- Front pressure of explosion shock wave: 50 kPa.
- Duration of compression phase: 300 ms.
- Direction of propagation is horizontal.
- Impact of a plane with 5.7 t mass at a speed of 100 m/s.

2.10.2. Loads on steel containment

- Effect of maximum excessive pressure: 0.4MPa, and maximum temperature: 134°C.

Size and energy of missiles inside the steel containment are determined in the design with regard to the "leak before break" concept. The mechanical effect of missiles and steam-water jets on the steel containment is excluded by means of a protective shield.

2.10.3. Steel containment protection against internal pressure

Leaktightness of the steel containment at maximum pressure of 0.43 MPa is to be such that leakage is not more than 0.3% of volume per day. During design accidents the confining safety system ensures confinement of radioactive material inside the steel containment, heat removal from the hermetic steel containment, and control and suppression of hydrogen.

2.11. Monitoring of plant safety status (4.2.3.9.)

2.11.1. Monitoring and identification of NPP safety status

The monitoring and control system provides an automated diagnosis of the state and the operating conditions of the NPP. Monitoring and presentation of information on the reactor coolant system, on all the safety-related systems, on the containment, on all operating conditions of the NPP and on remote control of these systems is provided. Post-accident monitoring system is provided to estimate the state of NPP.

Facilities for presentation of information including displays, for monitoring safety systems ensure:

- indication of control rod position
- monitoring of neutron flux during operation, refuelling and maintenance
- monitoring of level of radioactive contamination of the containment and the surrounding area
- preservation of adequate water level in the reactor vessel and the cooling systems
- emergency protection of the reactor
- protection of safety related systems.

2.12. Preservation of control capability (4.2.3.10.)

In case of a main control room failure, the reserve control room is to provide:

- reactor trip to hot shutdown condition
- maintaining of hot shutdown condition
- monitoring of subcriticality
- putting into operation of confining systems
- reactor cooldown with some local operations.

2.13. Station blackout (4.2.3.11.)

The normal and the emergency electric power supply system consists of two trains of 100% capacity, with each channel being divided into three groups considering reliability requirements and the time interval of loss of electric power.

Start-up of the two diesel-generators, one for each channel of reliable electric power and to be put into operation in the case of failure of main and reserve grid connections, is carried out for a period not exceeding 15 s from the moment of generation of a command to start-up.

D.C. electric power supply of the reactor control and protection system is ensured by accumulator batteries (in each train) designed for discharge over 24 hours. Electric power supply from accumulator batteries during blackout is provided for the main control room and the auxiliary control room in full measure.

2.14. Control of accidents within the design basis (4.2.3.12.)

Any intervention of operators during design basis accidents are prohibited for the first 30 minutes such that operators have enough time to consider the features of the accident occurred, and may prevent erroneous actions. Reactor safety is performed fully by the automatic control and protection system for the first 30 minutes. Reactor will arrive at walk-away safety.

In addition, provisions under design basis accidents are as follows:

- accident state monitoring, such as in-core and sump level monitoring
- indication of control rod position, including lights and digits
- indication of radiation level and radioactive releases
- monitoring of the reactor safety shutdown states

Hereabove systems are provided with automatic record devices during any accidents. Alarm light signals and digital indications are also provided in the central control room.

2.15. Mitigation and control of severe accidents

In order to prevent the core from melting or radioactive release from the plant to the environment, operators are required to utilize all of reasonable measures according to procedure H or U.

The fission chain reaction in the core should be stopped during severe accidents and the reactor returned to a controllable state. The measures of mitigation and accident management are researched through use of severe accident analysis.

3. EXTENDED DATA LIST

Station output

Rrated thermal power of reactor	1936 MW

Fuel assembly

Array	17 x 17 (AFA)
Number of fuel rods	38280
Number of guide tubes for absorber/in-core instrumentation	2900/40
Full length (without control spider)	4.10 m
Fuel rod, length	3.66 m
- outside diameter	9.5 mm
- cladding thickness	0.57 or 0.64 mm
- initial internal pressure (He)	3.06 MPa
Fuel pellet, material	UO_2
- density (percentage of theoretical density)	95.3%

Reactor core

Number of fuel assemblies	145
Active height	3.66 m
Equivalent diameter	2.92 m
Rod cluster control assemblies absorber	IN-Ag-Gd and stainless steel
Number of assemblies absorber rod per assembly	20
Enrichments, first core	1.9, 2.5, 3.1%
- reload	3.4%
(H_2O/UO_2) volume ratio	1.97
Average fuel burn-up	42000 MWd/t
Total weight of UO_2	66.8 t

Reactor Coolant System

Design conditions:	
- pressure	17.2 MPa
- temperature	343°C

Operating conditions:	
- pressure at vessel inlet	15.8 MPa
- pressure at vessel outlet	15.5 MPa
- temperature vessel inlet/outlet	293/327°C
Flow rate	47500 m^3/h
Heat transfer surface in core	6222.7 m^2
Average fuel linear rating	134.2 W/cm
Peak fuel linear rating	182.5 W/cm
Average core voluminal rating	78.69 kW/l

Reactor Vessel

Overall height with/without the head	12.22/9.92 m
Inside diameter	4.00 m
Wall thickness (opposite to the core)	205 mm
Inlet/outlet nozzle inside diameter	520.7/787.4 mm
Mass (including head)	390 t
Material (forged rings)	A508-III
Design pressure/temperature	17.2 MPa/343°C
Neutron fluence for service life	$< 2 \times 10^{19}$ n/cm^2

Reactor Coolant Pump

Type	canned
Number	4
Design pressure/temp.	17.2 MPa/343°C
Design flow rate	11875 m^3/h
Pump casing material	stainless steel
Speed	1500 rpm
Power at coupling cold/hot	3340/2545 kW
Weight	1.4 t
Coast down time	30 s
Pump motor inertia	0.15 t x m^2

Steam Generator

Type	Vertical U-tube
Number	2
Heat transfer surface	5430 m^2
Number of heat exchanger tubes	4474
Tube dimension	19.05 x 1.09 mm
Outside/inside diameter of shell	3.496/3.456 m
Total height	21 m
Transport weight	350 t
Tube material	Inconel-690
Shell and tube sheet material	A508-III
Steam pressure at SG outlet	6.65 MPa
Steam output	1951 t/h
Feed water temperature	230°C

Water volume of secondary side	164.1 m^3
Steam moisture at outlet from SG	≤0.25%

Pressurizer

Total volume	36 m^3
Steam volume full power / zero power	14.4/23.6 m^3
Design pressure/temp.	17.2 MPa/360°C
Heating power of the heaters	1440 kW
Number of heaters	60
Outside/inside diameter	2.33/2.1 m
Total height	11.0 m
Material	A508-III
Transport weight	90 t

Containment

Configuration (single or double)	double
Material	steel/concrete
Gross volume	50000 m^3
Pressure (design)	0.43 MPa
Height/diameter	57/37 m
Design leak rate	0.25 wt%/day

TECHNICAL INFORMATION ON DESIGN FEATURES OF APWR

K. Takumi
Nuclear Power Engineering Corporation, NUPEC,
Tokyo, Japan

I. Brief description of the concept

1. Introduction

The Advanced Pressurized Water Reactor (APWR) was developed in "The 3rd Phase·Improvement and Standardization Program for Light Water Reactors" of the Japanese government (MITI). The APWR builds on the current type PWR in Japan providing a reactor for the next generation to meet the national energy needs in the prospect that the dependance on the light water reactors as the stable energy supply source will continue for a considerably long period.

The APWR development program was jointly started and performed by the five Japanese PWR utilities including Kansai, Mitsubishi and Westinghouse as a seven party international cooperative development.

The improvement on plant availability, economics, maneuverability, safety, etc. was pursued in the program using the accumulation of the current PWR plant technology improvements obtained through the design, construction and operational experience. Various designs, tests and evaluations were performed based on the elaborately planned development program and the adequacy and reliability of major equipment were confirmed by the extensive tests from the design levels to the final verification levels.

In addition, the reliability of the reactor internals, fuel assembly and core components was verified as a whole in the tests called "Hydraulic Flow Test of APWR under Simulated Operating Condition" and "Verification Tests of Upper Core Internals for APWR" by the Nuclear Power Engineering Test Center (NUPEC) on commission of Ministry of International Trade & Industry (MITI).

Though the above mentioned APWR development program was started in 1982 and successfully completed in 1986 (fiscal year). After the development program, the upgrading program step 1 and step 2 continued to be performed aiming toward further advancement and rationalization, respectively.

Table 1-1 shows the history of the APWR development.

2. Features of APWR

Major Features on the performance of APWR are described below.

(1) Improvement on Availability

The APWR makes the long cycle operation of 13 to 18 months possible at lower fuel enrichment than that of the current PWR by the improved core design which adopts the spectral shift, large and low power density core, and it also shortens the in-service inspection time to 40 days. Therefore, the APWR can achieve an availability of more than 90% by those improvements.

(2) Improvement on Economics

The APWR reduces the fuel cycle cost about 20% by the adoption of the spectral shift, large and

Table1-1 APWR Development

Fiscal Year	1981	1982	1983	1984	1985	1986	1987	1988	1989
MITI	3rd Phase Improvement and Standardization Program								
Five PWR Utilities MHI Westinghouse		Development Study (Establishment of Basic Design) • Plant Design • Design Tests • Verification Tests				Upgrading Program (Step-1) • Improvement on Reactor Internals Endurance • Improvement on I & C Equipment Functions			
NUPEC (MITI)			Overall Verification Tests • Hydraulic Flow Test of APWR Fuel under Simulated Operating Condition • Verification Test of Upper Core Internals for APWR						
Kansai MHI								Upgrading Program (Step-2) • Improvement on Eqtipments • Reduction in Building Volume • Design Verification after Upgrading	

low power density core, radial reflector, and zircaloy grid fuel assembly. On the other hand, efforts are made to reduce overall plant capital costs. The APWR greatly reduces the electricity generation cost by these improvements and cost reduction efforts. Also, the APWR achieves a plant thermal efficiency of more than 35% by improving steam generator performance and by the adoption of 52-inch last stage blades in the low pressure turbine, etc.

(3) Flexible Siting

The APWR is designed to meet even the extremely high seismic requirementsand its electric power is increased to 1350 MWe to minimize the number of sites required. In addition, the building area per MWe is greatly reduced by its compact plant layout design.

(4) Improvement on Maneuverability

The APWR can provide load follow operation (from 100% to 50%, 14-1-8-1 hour cycle) without boron concentration adjustment and provide +5% automatic frequency control (AFC)/+3% governer free (GF) operation at the same time.

Table 2-1 shows the comparison of the major specifications between the APWR and the current 4-loop PWR.

3. Safety design

3.1 Basic Policy for Safety Security

The basic policy for the safety security of nuclear power plants is to secure the health and safety of the public in the surroundings and plant workers. The safety countermeasures are categorized as shown in the table below.

Safety Countermeasures	Example
○Accident Preventive and Effect Relief Countermeasures	
●Preventive Countermeasures to Occurrence of Abnormality	●Reliability Security of Equipment and System, etc
●Preventive Countermeasures to Expansion of Abnormality	●Safety Protection System, Inter-lock, Fail Safe, etc.
●Preventive Countermeasures to Releasc of Source Terms	●ECCS, Containment Vessel (CV), CV Spray, etc.
○Reducible Countermeasures to Public Radiation Exposure at Normal Operation	●Rad-waste Disposal System,etc.
○Security of Isolation between Plant and Public	●Site Selection agreed with Reactor Site Criteria

The APWR not only incorporates those safety countermeasures at each stage which has been considered in the current PWR but also makes improvements aimed at further enhanced reliability and safety. Those improvements are described below.

3.2 Countermeasures to Safety Improvement at Normal Operation

The APWR enhances its safety at normal operation by various improvements on the plant equipment and components reflecting the experience, know-how, etc. obtained in the current PWR.

Table2-1 APWR Plant Specifications

	APWR	Current PWR (4Loop)
Electrical Output	1350MWe	1180MWe
Thermal Power	3823MWt	3411MWt
Type of Turbine	TC6F52	TC6F44
Reactor Core	Spectral Shift by Mechanical Rods	—
Fuel Assembly	19×19array, 16thimbles	17×17array, 24thimbles
Control Rod Drive Mechanism		
CRDM & GRDM	Magnetic Jack Type	Magnetic Jack Type (CRDM)
DRDM	Hydraulic Piston Type	—
Reactor Vessel		
Inner Dia.	5m	4.4m
Total Height	16m	12.9m
Reactor Coolant System		
Number of Loops	4	4
Operating Pressure	157kg/cm^{2}G	157kg/cm^{2}G
Coolant Flow Rate	88,000m^3/hr	80,000m^3/hr
Steam Generator		
Heat Surface	6040m^2	4870m^2
Steam Pressure	69kg/cm^{2}G	61.5kg/cm^{2}G
Type of Containment	Prestressed Concrete or Steel	Prestressed Concrete
ECCS	4 Subsystems (2 Electrical Power Trains)	2 Trains

Major improvements in the APWR are as follows:

3.2.1 Fuel Assembly

The APWR fuel assembly reflects the achievement of the improvements in the reliability and load follow operation performance which have been applied to the current PWR fuel assemblies, and further enhances its loadability and mechanical reliability.

(1) Major Improvements

o For the fuel rods, the ratio of the clad thickness and outer diameter is increased for the enhanced PCI resistance performance and reduced fuel rod bow.

o Regarding fuel assembly grids, the number of grids is increased from nine to ten to increase the mechanical strength and further reduce fuel rod bow. Also zircaloy grids are applied to the intermediate grids for the enchanced neutron economics.

o The skirt is added to the top and bottom grids and all grid corner slopes are steepened and vanes and tabs are added to grids to enhance fuel assembly loadability and prevent grid damage.

o The leg type bottom nozzle is adopted to improve fuel assembly loadability.

(2) Design and Verification Tests

Many design tests and verification tests . were performed in APWR fuel assembly development and its reliability was confirmed.

Its final verification test: Hydraulic Flow Test of APWR Fuel under Simulated Operating Condition, which was performed by NUPEC, is explained below.

In the APWR, the coolant flow condition is different from that in the current PWR, because the fuel assembly with improved configuration is combined with water displacer rods (WDR) and WDR drive mechanism. (DRDM) unique to the APWR. This flow test was performed under high pressure and temperature condition to verify the overall mechanical integrity of the WDR drive line channel which consists of DRDM, WDR, reactor internals and fuel assembly.

In this test, the actual assembly flow was duplicated in the pressure vessel of the high pressure and temperature hydraulic test loop in which a fuel assembly, a WDR cluster, a WDR rod guide, and a DRDM of full scale were installed.

This test consists of the following test items.

(i) Vibration Characteristics Test
(a) Measurement of Fuel Rod Vibration
(b) Measurement of WDR Cluster Vibration
(c) Measurement of WDR Rod Guide and Calandria Tube Vibration

(ii) Hydraulic Characteristics Test
(a) Measurement of Fuel Assembly Pressure Loss and Lift Force
(b) Measurement of WDR Rod Guide Pressure Loss

(iii) Functional Test of WDR Drive Line
(a) WDR Cluster Withdrawal and Insertion Test
(b) DRDM Driving Function Characteristics Test

(iv) Endurance Test
(a) Repetition Test of WDR Cluster Withdrawal and Insertion
(b) Long Period Operation Test (1,000 hours)

The results of the test on the fuel assembly are described below.

(i) Fuel Rod Vibration Characteristics Test

The flow-induced vibration of fuel rods was small and no abnormal vibration was observed.

(ii) Fuel Assembly Hydraulic Characteristics Test

- o The actual pressure loss measured in the test was significantly less than the expected loss.
- o It was confirmed that the fuel assembly lift force was small and the starting point of the lift caused by the flow was more than the rated flow.

(iii) Fuel Assembly Inspection after Test

- o Fuel rod wear after the long period operation (1,000 hours) was small and its wear depth during the life was considerably smaller than the restricted value.

The integrity of the fuel assembly under all operating condition was confirmed by the results mentioned above.

3.2.2 Reactor Internals

The APWR reactor internals have the configuration which meets all the requirements of the spectral shift and large core unique to the APWR in addition to the fundamental functions to support the core, to form the coolant flow channel, and to guide and support the control rods, which are common to the current PWR. Also, the APWR reactor internals enhance safety and reliability.

(1) Major Improvements

- o The upper calandria is adopted to the upper core internals of the APWR. In the current PWR, the coolant ascending from the core changes its flow toward the reactor vessel outlet nozzle in the control rod guide region. In the APWR, however, the calandria is installed above the rod guide region to allow the coolant at the core outlet to ascend vertically in the rod guide region and to change its flow to the lateral direction in the calandria. This configuration improves the integrity of control rods by reducing flow-induced vibration.

- o The radial reflector is adopted in place of the core baffle, former and thermal shield which are used in the current PWR. This enhances the neutron economics and reduces the neutron radiation to the reactor vessel while improving fuel economy.

(2) Configuration of APWR Reactor Internals

(i) Upper Core Internals

The APWR upper core internals consist of the core barrel, RCC (Rod Cluster Control)/GR (Gray Rod)/WDR rod guides and calandria assembly. The calandria assembly consists of the calandria tubes, their upper and lower plates, and shell. The flow ascended vertically in the rod guide region is allowed to flow toward the outlet nozzle in the calandria. WDR rod guide consists of an enclosure with an octagonal section and RCC/GR rod guides consist of an enclosure with a cruciform section from the results of the various studies on the strength, manufacturability, etc.

(ii) Radial Reflector

The radial reflector configuration adopted consists of a thick stainless steel box in which round stainless steel bars are contained based on the results of studies on the neutron reflection effect, effect of the reduction in the neutron radiation to the reactor vessel, manufaturability, etc.

(3) Design and Verification Tests

Many design tests and verification tests were performed in the APWR reactor internals development and confirmed these component reliability.

"Verification Test of Upper Core Internals for APWR" which was performed by NUPEC, and "Radial Reflector Hydraulics Test" are explained below.

(i) Verification Test of Upper Core Internals for APWR

This flow test was performed to obtain the actual hydraulic characteristics and to confirm the overall resistance to flow-induced vibration for the APWR upper core internals. This test was performed in a pressure vessel in which a 45°-sector upper core internals model of full scale and a 90°-sector calandria model of half scale were installed under the medium temperature and pressure condition similar to the actual condition in respect to the fluid dynamics.

The integrity of the APWR upper core internals to the flow induced vibration and hydraulic loads was confirmed from the results of this test.

(ii) Radial Reflector Hydraulic Test

This flow test was performed to confirm the flow condition in the circumference of the core where the radial reflector was installed and the resistance of the radial reflector and adjacent fuel rods to flow induced vibration. This test was performed under the low pressure and temperature condition, using a radial reflector module and a fuel assembly of full scale.

The absense of flow-induced vibration in the radial reflector and adjacent fuel assembly was confirmed by this test.

3.2.3 STEAM GENERATOR

Since the steam generator is a very important component which determines the reliability of the PWR plant, extensive efforts have been made in the past to improve its reliability.

Initial steam generator materials and manufacuring methods experienced various troubles related to the integrity of the tubes. But the technology has been improved since then, and the materials and design for the steam generators in the plants which started operation in the recent years were modified sufficiently and reliability has been enchanced.

However, improvements still continued in the APWR development and further enhanced reliability was pursued thoroughly to produce better steam generator.

Major improvements on APWR steam generator are as follows:

o Tube made of TT690 alloy, which has the best resistance to corrosion in the primary and secondary environments, is adopted.

o Improved Broached Egg Crate (BEC) type tube hole to support the tube is adopted. This type of hole is equivalent to conventional BEC type hole in corrosion resistance, and has better strength than that of conventional one.

Many design tests and verification tests were performed in the APWR steam generator development and its reliability was confirmed.

"Steam Generator Tube Material Development Test" and "Steam Genetator Tube Support Development Test" are explained below.

(1) Steam Generator Tube Material Development Test

Since the tube material selection is the most important for the reliabiity of the steam generator, various kinds of candidate materials were carefully examined and evaluated under the extensive development test program. As the results of overall evaluation, TT690 alloy was selected for its SCC resistance under the primary environment and its IGA/SCC resistance (particulary in alkaline condition) under the secondary impurities environment.

(2) Steam Generator Tube Support Development Test

The impurities concentration test at the tube support plate crevices were performed for the grid type and improved BEC type tube support plates. As the result of the test, it was confirmed that the improved BEC type had excellent performance.

3.2.4 Instrumentation and Control System

The APWR I&C features the fully micro-computerized processing system that involves even the protection system, and it offers enhanced safety, reliability and maintainability. The advancements of the APWR I&C system compared with that of the current PWR are as follows·

o Increased Operational Margin by Improvement of Processing Capability and Accuracy

o Easy Detection of Failure by Self-diagnostic Capability and Enhanced Maintenability with Automatic Testing Capacility

o Enhanced Reliability by Increased Redundancy of Control System

Regarding the automation, the systems which have emergency needs or wide area of operation during normal operation or abnormal/accident operation have been automated in the past, and the human-error and operators' loads have been reduced. In addition to this, automation of operations during plant start-up and shutdown, which require a number of actions and surveillance, is planned.

3.2.5 Control Room

The design of the control room is planned to include additional human factors design and color coordination in the control room, etc. to improve the operators' man/machine interface.

The hardware equipment such as the switch display lamp, etc. on the control board which have been used in the past are removed from the control board and are put on to CRT screens. CRT display design as well as cabinet layout design use modem human engineering methods. Operator surveillance and control of plant systems and components are integrated in CRT displays.

Regarding the operation support, the operations guidance system during abnormal/accident conditions and the improved alarm display system, in which the color of the alarm windows is changed in accordance with their importance, are used so that the recognition of the alarm and its consequences are made easy.

3.2.6 Layout Design

The layout design is improved so that the equipment layout will enhance the reliability of the nuclear power plant, minimize the effect of accident or failure, and ensure that equipment will be safe and easy to use.

In the APWR, the engineered safety pump compartments are located independently in separate safeguard areas by utilizing the features of 4 subsystem primary side safeguards system, and the emergency water storage tank (EWST) is located in the containment vessel Also this layout effectively utilizes the space in the buildings. Further, the slide layout of the buildings and equipment between each plant unit is applied and the color tone of the floors, walls and doors are selected to prevent misunderstanding the units. These carefull considerations improve the operators' reliability.

3.3 Improvement Countermeasures to Safety at Accident

The new type primary side safeguards system: Integrated Safeguards System (ISS) was developed in the APWR by concentrating the safety design technology which has been improved in the past and the ISS enhances safety and reliability.

The major improvements on ISS are described below.

(1)The adoption of 4 subsystems eliminates the tie-line and branched piping of each subsystem, improves the redundancy/independency, enhances the reliability, and simplifies the system configuration.

(2)The emergency water storage tank (EWST) is installed at the bottom of the containment vessel and is utilized as the water source for the engineered safety pumps. Thereby, the operators' action after an accident is reduced and the reliability is enhanced, because switch over for recirculation which is required in the current PWR is not necessary. Since EWST can be used to fill the water into the reactor cavity when the refueling is carried out, the refueling water storage tank in the current PWR can be deleted, so it also contributes to the simplification of the system.

(3)The core reflood tank which is installed as passive equipment instead of the low pressure injection system in the current PWR simplifies the system configuration and enhances the reliability.

4. Conclusion

The APWR development was the largest scale development conducted for the light water reactors in Japan. This five year development program has been completed and has successfully accomplished the objectives.

Hereafter, further advancement will be pursued on the basis of this development accomplishment.

II. Description of key features in 15 design areas

1. Plant process control systems

(1) There are provided the necessary nuclear and process instrumentation required for normal operation and protection action such as neutron flux, temperature, pressure, water level, flow rate and so on. And the reactor control systems are provided in order to automatically control the reactor in case of design load changes.

(2) The reactor control systems are designed as follows.

i. Reactor power is followed by turbine load at normal operation.
ii. The plant is controlled so that main plant and system variables remain within their acceptable ranges and their response becomes stable with enough damping ratio.
iii. The operators are able to monitor the status of the plant conditions and manually control plant if necessary.

(3) The reactor control systems are composed of the following sub-systems.

i. control rods control system
ii. boron concentration control system
iii. pressurizer pressure control system
iv. pressurizer water level control system
v. feed water control system
vi. turbine bypass control system
vii. main steam relief valve control system
viii.rod withdrawal block and turbine run back

(4) When abnormal conditions or troubles occurred at normal operation,operators could monitor automatically the plant variables such as neutron flux, temperature, pressure, radioactivity and so on. And the interlock systems are provided so that

errors and mis-operations would not result in reaching to abnormal conditions and accident conditions.

2. Automatic safety systems

(1) Automatic safety systems are provided that would safely shut down the reactor, maintain it in a cooled state and limit any release of fission products, if various anticipated abnormal transients and accidents occurred.

(2) In order to attain above functions, multiple reactor trip signals and engineered safe guard system actuation signals are provided. Engineered safe guard systems include emergency core cooling system,reactor containment vessel isolation valves,reactor containment spray system and so on.

(3) Automatic safety systems are designed to have redundancy and independency and fulfill their safety function ,if single failure of system occurred. And they are able to be tested to perform their safety functions during normal operation or refueling shutdown.

3. Protection against power transient accidents

(1) The reactor core is designed so that reactor power could be sufficiently suppressed by its inherent negative reactivity feedback characteristic which consists Doppler coefficient, moderator temperature coefficient, moderator void coefficient and so on, if abnormal transients with rapid increase in reactivity occurred at normal operātion.

(2) As reactor shutdown systems, there are provided two independent systems which mechanism is different, one is insertion of reactor control rods clusters by reactor control rods control system and another is injection of boric acid by chemical and volume control system.

(3) The reactor control rods clusters are designed so that the reactor could be subcritical at hot condition by insertion of the reactor control rods clusters, if one reactor control rods cluster which has the largest worth was stuck at the fully withdrawal position and not able to be inserted into the reactor core.

(4) The chemical and volume control system is designed so that the reactor could remain sufficiently subcritical at both hot and cold condition including xenon build up condition, by injection of boric acid into the core.

4. Reactor core integrity

(1) The fuel assemblies are designed so that each element of assembly could have enough strength and maintain its mechanical function under both normal operation and anticipated abnormal transient condition. Further they are designed not to affect the function of non fuel bearing components.

(2) Fuel rods are designed to satisfy the following criteria under both normal operation and anticipated abnormal transient condition.

i. Maximum temperature at the center of fuel rod shall be under the melting point of UO2.

ii. Inner pressure of fuel rod shall not exceed the normal operation pressure of the reactor coolant.
iii. Stress of fuel cladding shall not exceed the proof stress of the cladding material.
iv. Deviation of circumferential tensile strain of fuel cladding shall not exceed 1% in case of each transient
v. Cumulative fatigue cycles shall be within the limit of design fatigue life.

5. Automatic shutdown systems

(1) Safety shutdown systems are fundamentally independent in function from the reactivity control systems used for normal operation. If the signals of the instrumentations from the safe shutdown systems are also used for the plant process control systems, isolation amplifiers are provided at the branch of signals so that troubles such as shortage or break of circuits of the output side (the plant process control systems) would not affect the function of the input side (the safe shutdown systems).

(2) The plant is designed so that the probability of ATWS is sufficiently low and the probability of large amount of fission products release to public is as low as possible.

6. Normal heat removable

(1) The plant is designed so that heat of the reactor is removed by steam generators at normal operation and early phase after reactor shutdown. This steam from the steam generators is either cooled by the turbine condensers or released to the atmosphere through the atmospheric relief valves. After pressure and temperature of reactor coolant become lower than the predetermined value ,residual heat removable systems are provided to remove the residual heat of the core.

(2) Residual heat removable systems are designed so that temperature of reactor coolant can be decreased to 60° C within around 20 hours after reactor shutdown ,using all trains of the systems.

(3) Assuming that heat removable from the reactor using the secondary side is necessary at accident conditions , the plant is designed so that heat of the core could be transported to the secondary side through the steam generators by forced convection or natural convection of reactor coolant. Auxiliary feed water systems and atmospheric relief valves and main steam safety valves are provided for feeding water to the steam generators and releasing steam from SG at abnormal conditions.

(4) Above heat removable systems are designed to have redundancy and the active components such as auxiliary feed water pumps and residual heat pumps are designed to be power-supplied through emergency busses.

7. Emergency heat removable

(1) Emergency core cooling systems are designed so that serious damage of fuels and fuel cladding could be protected and reaction between cladding metal and water could be limited to the sufficiently small amount.

(2) Emergency core cooling systems are composed of accumulator injection systems, high head injection systems and low head injection systems. Accumulator injection

systems and low head injection systems are designed to start injection to the core by automatic opening of check valves when pressure of reactor coolant becomes below the operating pressure of accumulators and core reflood tanks. High head injection systems are designed to automatically start by ECCS actuation signals and be power-supplied through emergency busses in case of blackout condition.

(3) Emergency core cooling systems are designed to have independency to be able to attain required safety functions without off site power , if single failure of active components occurred until finish of injection mode after accident occurrence, and single failure of either active components or passive components occurred.after that.

(4) Emergency core cooling systems are designed so that periodical tests and inspections could be available for each independent system to verify their integrity and redundancy.

8. Reactor coolant system integrity

(1) The reactor coolant pressure boundary is designed taking attention to selection of material, seismic strength, over pressure protection and so on so that the probability of abnormal leakage of reactor coolant and break of pressure boundary would be extremely small. And it is also designed so that inservice inspections could be available to verify its integrity.

(2) The pressure and temperature of the reactor coolant pressure boundary is designed to remain within the limited range at all the anticipated operating conditions by means of primary reactor coolant systems, engineered safeguard systems, reactor auxiliary systems, instrumentation and control systems and so on. The components such as reactor vessel, pressurizer, steam generators are verified to have enough strength by analysis considering each anticipated transient conditions.

(3) Instrumentations such as radiation monitors are provided to quickly detect the leakage of reactor coolant from the reactor coolant pressure boundary. If these instrumentations detected abnormal conditions, operators could realize the status of the plant by means of annunciators in the control room.

(4) The reactor coolant pressure boundary is designed to avoid brittle characteristic and rapid propagation type of destruction. Therefore, for ferritic steel vessels, careful attention is paid to material, design, fabrication and operation. From the standpoint of preventing brittle failure of components, heat-up and cool-down rate is controlled to be within a limited value and also operating temperature is controlled to be more than pre-determined minimum value of material. For the reactor vessel, surveillance test pieces installed in the reactor vessel are periodically taken out in order to confirm the lowest operable temperature which is increased by the neutron radiation.

(5) The neutron radiation to the APWR reactor vessel could be reduced to less than a half amount of .that of conventional PWR due to newly adopted 48 radial reflector modules made of stainless steel rods which are installed at the core periphery. And a forging ring is used for the core region of the reactor vessel so that weld lines can be deleted in the core region and both integrity and inspectability could be enhanced.

9. Confinement of radioactive material

(1) The reactor containment vessel is designed so that it can withstand the high internal pressure and high temperature caused by release of reactor coolant in case of the anticipated loss of coolant accidents, together with the containment spray system which is capable of reducing the inner pressure and temperature and minimizing release of fission products to the circumstance.

(2) The reactor containment vessel is designed to be capable of conducting leak rate tests to verify that the total leak rate would not exceed the design value.And out of the penetrations, the electrical penetrations, air-locks and so on, are designed to be able to conduct leak test or leak rate test individually or in small groups.

(3) The annulus clean up system and the containment spray system are provided to reduce radioactivity release to the circumstance at the accidents. The annulus clean up system is designed to remove iodine in the gas which leaks from the reactor containment vessel at the accidents. The containment spray system is designed to reduce the concentration of iodine in the gas released to the CV, as well as to actuate as containment heat removable system at the accidents.

10. Protection of confinement structure

(1) The plant is designed to reduce the probability of occurrences of severe core accidents to the extremely low level. Therefore, severe core accidents are not considered to be design basis accidents.

(2) Study on improvement of the mechanical integrity of the reactor containment vessel and several mitigation measures at the severe core accidents is on going.

11. Monitoring of plant safety status

(1) Various kinds of plant variables required for operation at the accidents are designed to be monitored in the control room. It is important to detect rapidly the abnormal condition, because operator action in the early phase of the accidents might protect the expansion of the abnormal conditions to the accidents. From this point of view, loose parts monitors, vibration / noise monitors, leak detectors, radiation monitors, thermometers and so on are provided to be monitored in the control room.

(2) From the view point of enhancing man-machine interface, the main control panels are designed to be console type and be capable of monitoring and operating only on the screen of CRTs, so-called touch screen type. Adopting such design could supply selected plant variables in an intensive manner to the operators at the accidents.

12. Preservation of control capability

(1) Cables and control panels are. designed to be made of noninflammable or almost noninflammable material as far as practical, so that the probability of occurrence of fires in the control room would be extremely low.

(2) The control room is designed so that the operators could remain there and conduct necessary actions , if the accidents occurred, by means of the provisions of the appropriate shield and the heating and ventilation systems.

(3)If the operators could not remain in the control room for any reason, the plant is designed so that the operators could shutdown the reactor safely. The operators could shutdown the reactor rapidly by means of either opening the reactor trip breakers in the control rod drive mechanism electrical power panel room, or tripping the turbine at remote location. Further, an alternative panel somewhere outside the control room is provided so that the operator actions could be taken for the components which are often used for the hot standby operation or are used for the short period after the reactor trip and minimum plant variables required for this operator action could be available.

13. Station blackout

(1) As electrical power supply to the station, in addition to the off-site power strongly connected to the grids, there are provided two trains of emergency diesel generator systems which supply power to the emergency busses.Therefore, the probability of loss of electrical power supply even in the limited period would be extremely low. However, if short time station black out occurred, the reactor could be safely shut down by means of the actuation of the reactor safe shutdown systems. Further, heat removable of the core could be attained by means of both natural convection of the reactor coolant in the primary side and actuation of the turbine driven auxiliary feed water pumps and main steam safety valves in the secondary side.Electrical source of the reactor safe shutdown systems and the turbine driven auxiliary feed water systems would be supplied from the highly reliable battery.

14. Control of accidents within the design basis

(1) There are provided the plant control systems and automatic safety systems so that the plant could be returned to the normal condition if abnormal conditions occurred, and the reactor could be shut down and large release of fission products could be protected if the accidents occurred. And the operating procedures required for the above abnormal and accidental conditions are clarified and reflected into the plant design.

(2) If manual operations were required, the plant is designed so that more than 10 minutes would be available for the operators to realize the plant status precisely and to be confident of that the operator manual action would not affect the control of the abnormal conditions and accidents.

15. Mitigation and control of severe accidents

(1) The plant is designed to reduce the probability of occurrences of severe core accidents to the extremely low level. Therefore, severe core accidents are not considered to be design basis accidents.

(2) Study on improvement of the mechanical integrity of the reactor containment vessel and several mitigation measures at the severe core accidents is on going.

III. List of main parameters

ELECTRIC POWER	1350MWe
Core Power	3823MWt
Fuel Assembly	
Array	19 x 19 lattice
Number of fuel rods	296
Number of thimbles	16
Fuel rod cladding material	Zircaloy 4
Reactor Core	
Number of fuel assemblies	193
Active height	3.9m
Equivalent diameter	3.98m
Total weight of U	119.2t
Number of rod cluster control assemblies(RCC)	69
Number of grey rod cluster control assemblies(GRC)	28
Number of water displacer rod cluster control assemblies(WDR)	88
Material of RCC	Ag-In-Cd + B4C
Material of GRC	Stainless Steel
Material of WDR	Zircaloy
Reactor Coolant System	
Number of loops	4
Coolant pressure	157kg/cm2g
Cooolant flow	88,000m3/hr
Reactor Vessel	
Inside diameter	5m
Overall heigt	16m
Reactor Coolant Pump	
Number	4
Flow rate	22,000m3/hr

Motor horse power	8000HP
Steam Generator	
Number	4
Heat transfer surface	6039m2
Tube material	TT690 alloy
Steam pressure	69kg/cm2g
Pressurizer	
Total volume	71m3

TECHNICAL INFORMATION ON DESIGN FEATURES OF MS-600

K. Takumi
Nuclear Power Engineering Corporation, NUPEC,
Tokyo, Japan

I .Brief description of the concept

1. Introduction

The next generation of light water reactor is being developed worldwide today. These developments include the application of so-called passive safety components which use natural phenomenon for their driving force. Passive safety components and systems are being considered for adoption in place of conventional safety systems using mainly active components, as a way of further improving the safety of nuclear power plants, by achieving the following targets;

○ Simplify safety systems and improve their reliability and cost
○ Reduce the demands on the operators and avoid human factor errors which sometimes affect operations during accidents
○ Provide sufficient time margins to enable the operators to cope with accidents

Mitsubishi has succeeded in applying this passive safety concept at the system level with the detailed consideration on its limitation and has now developed hybrid safety systems. We are expecting that hybrid safety systems will be applied to the next generation of plants.

The hybrid safety systems studied in the first place are intended for use on a 2-loop PWR plant with an output of 600MWe class which is called the MS-600. Because the main feature of the MS-600 is in its safety systems, the design concept of the hybrid safety systems are mainly described hereafter.

2. Safety Design

2.1 Structure of the hybrid safety systems

In developing the new concept of hybrid safety systems, we first of all analyzed and assessed the advantages and disadvantages of each type of safety systems.

One of the advantages of active safety systems is their effectiveness in terminating an accident quickly and in preventing the expansion of accidents. They also provide operational flexibility under different accident conditions, and they can be used in the best way and in the best combination according to the operator's judgment.
Their disadvantages are the possibility of aggravating an accident by operational errors or misunderstandings on the part of the operators, and the complexity of the systems which require a series of active components including sources of power to operate correctly.

Passive safety systems are simple, highly reliable and allow the designer to eliminate human errors which sometimes make accident situations worse, because they are totally composed of passive components which utilize natural forces and do not require operator actions or a series of operations of peripheral components. On the other hand, when passive safety systems are employed, it takes a long time to terminate an accident and the operation procedure is fixed so that, in some cases, even a small accident finally results in flooding the inside of the containment, which requires a tremendous restoration effort.

The hybrid safety systems rely on the passive safety systems to handle LOCAs which are highly unlikely to occur. As for more likely non-LOCA events, such as blackout or failures of secondary system piping, or steam generator tube ruptures (SGTR), or breakage of primary system piping with a diameter equal to or less than 1 inch (very small-size LOCA), they are dealt with by active safety systems, and the passive safety systems act as a backup for the prevention of core damage if the active safety systems do not operate correctly due to operational errors or for some other reason. Such an optimum combination can improve safety while maintaining the advantages inherent in the present systems (Fig. I -1).

2.2 Operation procedure of hybrid safety systems

The operation of the hybrid safety systems is described below and is shown diagrammatically in Fig. I -2.

2.2.1 Active safety systems

The active safety systems consist of charging/safety injection pumps, auxiliary feedwater pumps and their power sources. The operating procedure for them are the same as those of a conventional plant but they have a more limited set of functions and a reduced number of roles to play in comparison with the conventional ones so the systems have become simpler.

2.2.2 Passive safety systems

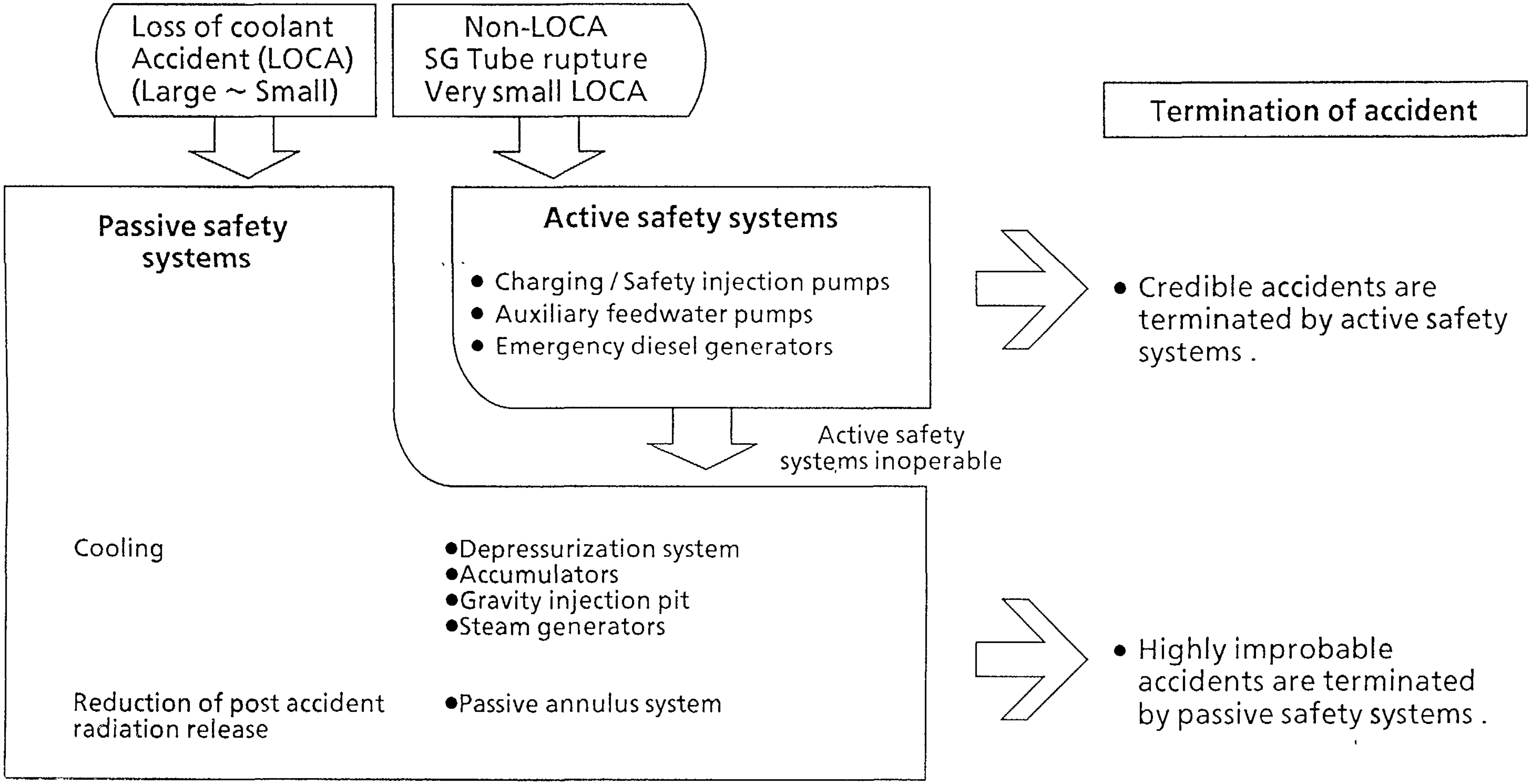
When a LOCA occurs, it causes a pressure drop in the primary system, and if it drops below a set point level, the primary depressurization valves of the pressurizer will open followed by the secondary depressurization valves in the main steam lines, thus forcefully reducing the pressure both in the primary and secondary systems.

In the first stage of the accident, water from the accumulators which are pressurized to about 5MPa., is injected into the reactor core, and when the primary system pressure drops to a pressure close to that of the containment, a large amount of water from the gravity injection pit will be injected by gravity thus maintaining cooling.

In the meantime, when the pressure in the secondary side of the steam generators is reduced, water is injected from the condensate storage tank by gravity and is then evaporated in the steam generators and the steam is released from the secondary depressurization valves. Heat is thus removed from the primary system by the steam generators.

Reactor core cooling can be maintained in this way for several hours and during this time water spilling out of the break will accumulate inside the containment vessel.

After the Reactor Coolant Loop is submerged, decay heat will be transferred to the steam generators by natural circulation, and discharged to the



Loss of coolant Accident (LOCA) (Large ~ Small)

Non-LOCA SG Tube rupture Very small LOCA

Termination of accident

Passive safety systems

Active safety systems

- Charging / Safety injection pumps
- Auxiliary feedwater pumps
- Emergency diesel generators

- Credible accidents are terminated by active safety systems .

Active safety systems inoperable

Cooling

- Depressurization system
- Accumulators
- Gravity injection pit
- Steam generators

Reduction of post accident radiation release

- Passive annulus system

- Highly improbable accidents are terminated by passive safety systems .

Fig I -1 Concept of hybrid safety systems

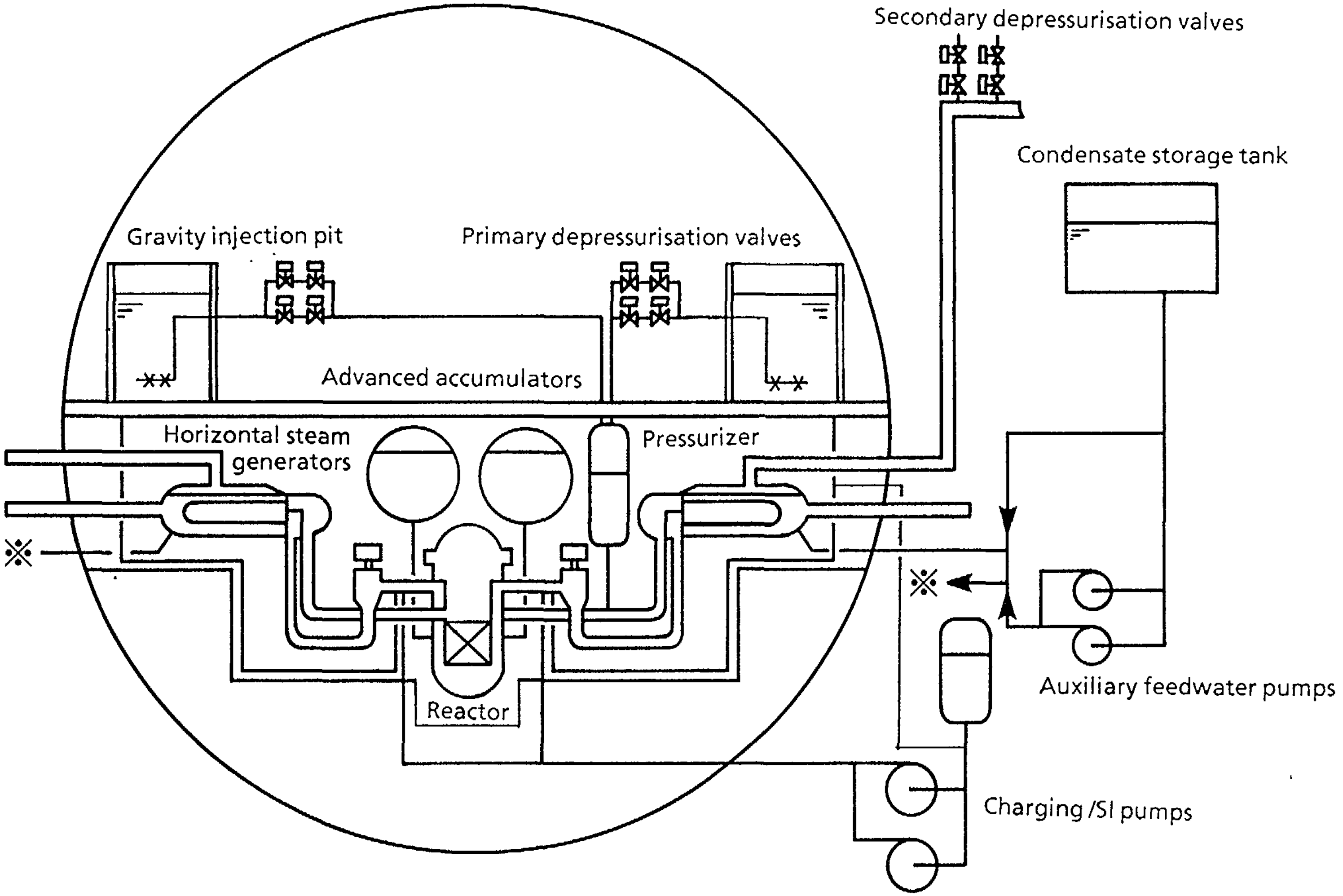

Secondary depressurisation valves
Condensate storage tank
Gravity injection pit
Primary depressurisation valves
Advanced accumulators
Horizontal steam generators
Pressurizer
※
※
Reactor
Auxiliary feedwater pumps
Charging /SI pumps

Fig Ⅰ -2 Configulation of hybrid safety systems secondary side. The condensate storage tank has a capacity equivalent to 3 days of decay heat so reactor core cooling can be continued for 3 days without requiring any operator action. After this period, cooling can be continued either by supplying water to the condensate storage tank or by using other safety systems which can now be operated, or by normal active components.

2.3. New design and development items for the hybrid safety systems

For the passive safety systems, there are some new concepts, and it was necessary to develop several items which are not found on existing plants.

2.3.1 Development of advanced accumulator

During a LOCA, a large amount of cooling water has to be provided to the core quickly in the early stage to reflood the vessel, and then a relatively small amount of water should continue to be injected into the core to quench it and remove decay heat.

The advanced accumulator is provided with a vortex flow control device located in the discharge nozzle which controls the flow, using the principle shown in Fig. I -3.

When the water level in the accumulator is above the top of the main flow standpipe, water enters the vortex chamber through both inlets and as the flow is smooth, a large flow of water is discharged(Fig. I -3, situation (a)). When the water level drops below the top of the main flow standpipe, however, the water enters the vortex chamber only through the side connection which is tangential to the chamber. This causes a vortex which increases the flow resistance and the flow rate is reduced (Fig. I -3, situation(b)).

The feature of this system is that the flow of water can be changed with a simple and passive device, without using any active components such as valves.

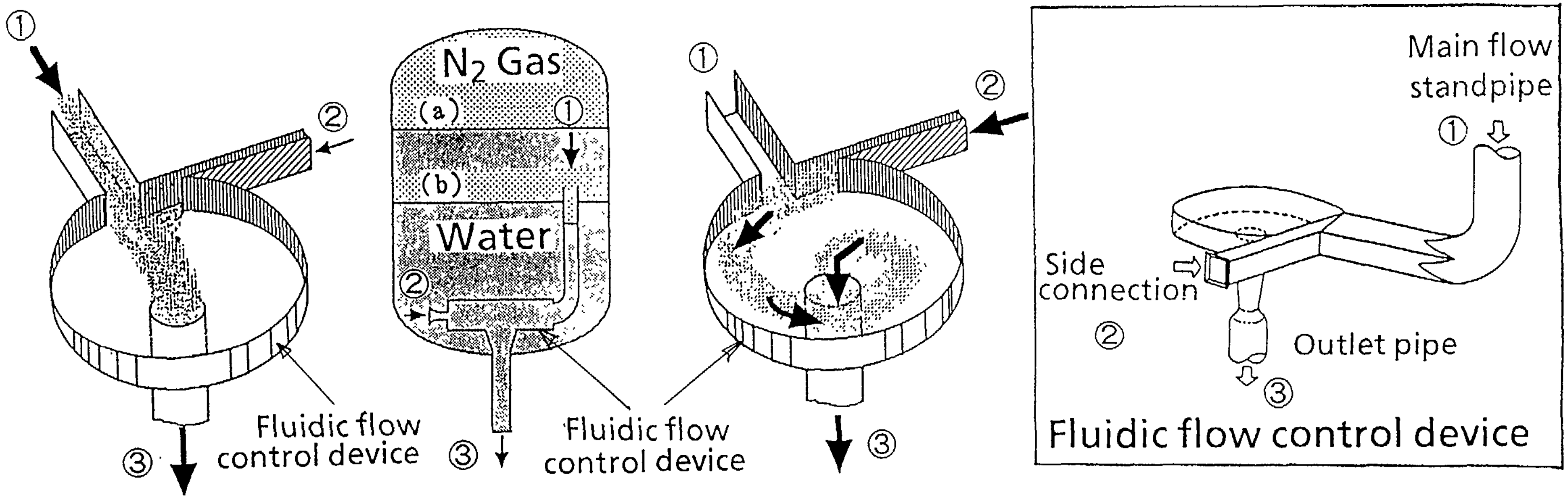
2.3.2 Development of passive core cooling system

This system utilizes the steam generators for core cooling and the decay heat in the reactor core following a LOCA is transferred to the steam generators by natural circulation in the primary system. However, in order to avoid a possible siphon break caused by the accumulation of non-condensible gas in the steam generator tubes, the steam generator is designed to be horizontal as shown in Fig. I -4. Non-condensible gas will be removed from a vent line on the channel head of the steam generators instead of entering the tubes.

The horizontal steam generator is a new design and, compared to a conventional vertical one, sludge is less likely to accumulate on the tube plate during normal operation. This type is also more resistant to earthquakes because of its low height. Detailed studies of this design are continuing.

2.4. Safety and protection logic of the hybrid safety systems

It is important to make sure that the systems will surely operate when required but, in addition to that, if plant safety can be guaranteed sufficiently by the active safety systems, unnecessary actuation of the passive safety systems should be prevented to avoid the longer plant recovery time involved. Also, since it is intended to deal with SGTRs by automatic active safety systems which require no operator action, signals for this purpose will also be needed.


①
②
③
Fluidic flow control device
N_2 Gas
(a)
①
(b)
Water
②
③
Fluidic flow control device
①
②
③
Main flow standpipe
①
Side connection
②
Outlet pipe
③
Fluidic flow control device

(a) Large flow rate (Smooth flow)

(b) Reduced flow rate (Reduced flow by vortex resistance)

Fig I -3 Principle of the advanced accumulator

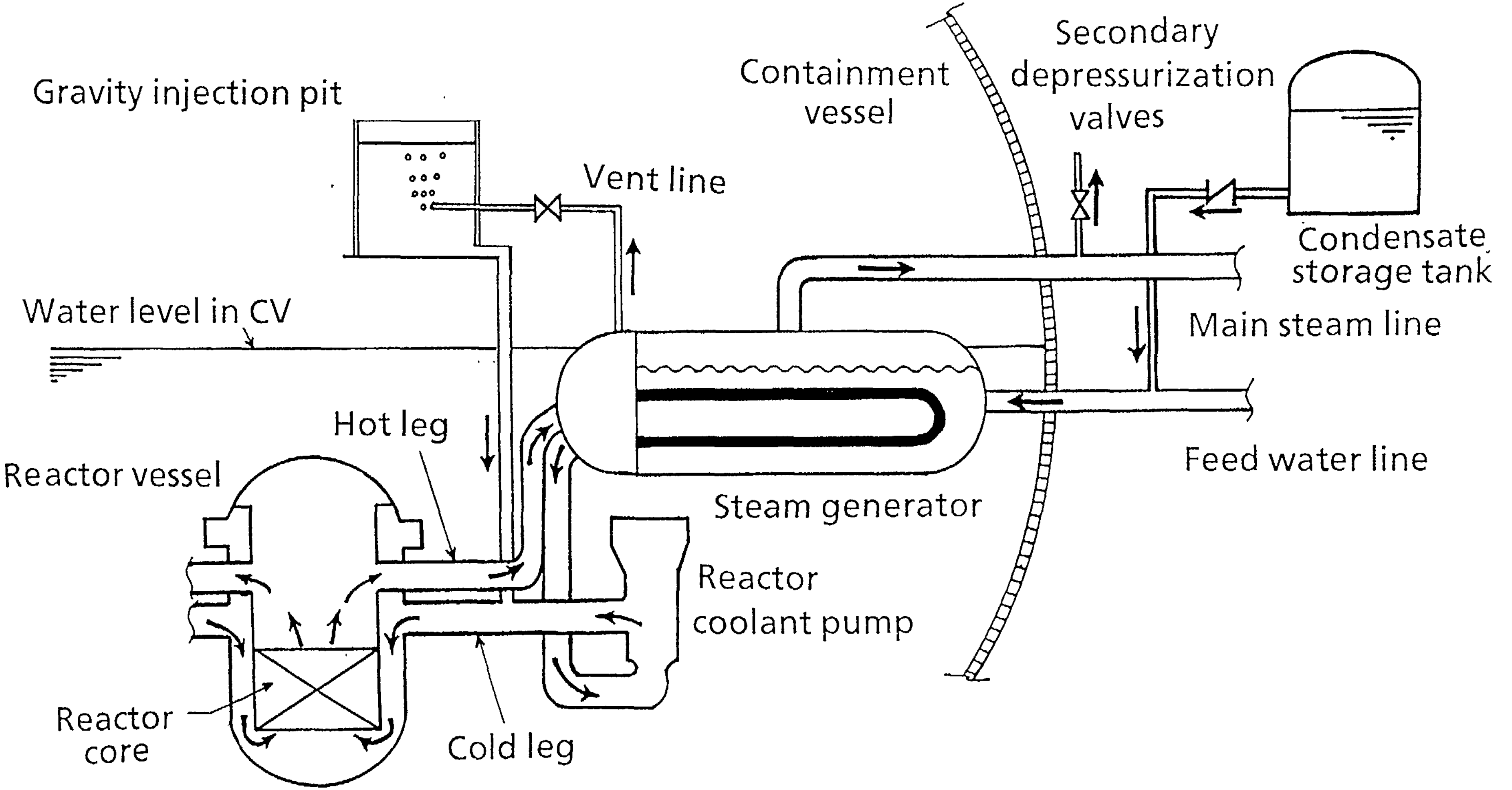


Fig I -4 Steam generator cooling system

The secondary depressurization system should not open immediately after the start of a LOCA but only after the primary depressurization system has actuated. This is to prevent a large reduction in the water inventory of the steam generator secondary side. A distinction is made between a primary system pressure reduction due to a line break in the secondary system and one due to a LOCA by judging whether the secondary system pressure as well as the primary system pressure is dropping rapidly or not. Also, judgment of the occurrence of a SGTR is made from the indication of the main steam line radiation monitors. At present, two types of reactor vessel water level measurement systems are under discussion for possible application in the identification of accidents.

2.5. Safety analyses

As part of our effort to achieve a high level of safety, we have been carrying out safety analyses from the early stages of the conceptual design. At this stage, the important matter is to confirm the suitability of the hybrid safety systems by safety analyses. As for the initiation events, there is nothing especially different from those of conventional plants.

To be more specific, we have performed as the most urgent tasks the analyses to confirm that reactor cooling and the safety of the containment vessel can be maintained during a LOCA by the use of the passive safety systems alone and to confirm the suitability of the safety and protection logic for non-LOCA events which is different from that of conventional plants.

We have also concluded that it is important to apply probabilistic safety assessment (PSA) as much as possible from the early stage of the basic design in order to cover multiple accident conditions beyond the design expectations and to achieve a safety level exceeding that of a conventional plant, and have performed it for main accident sequences.

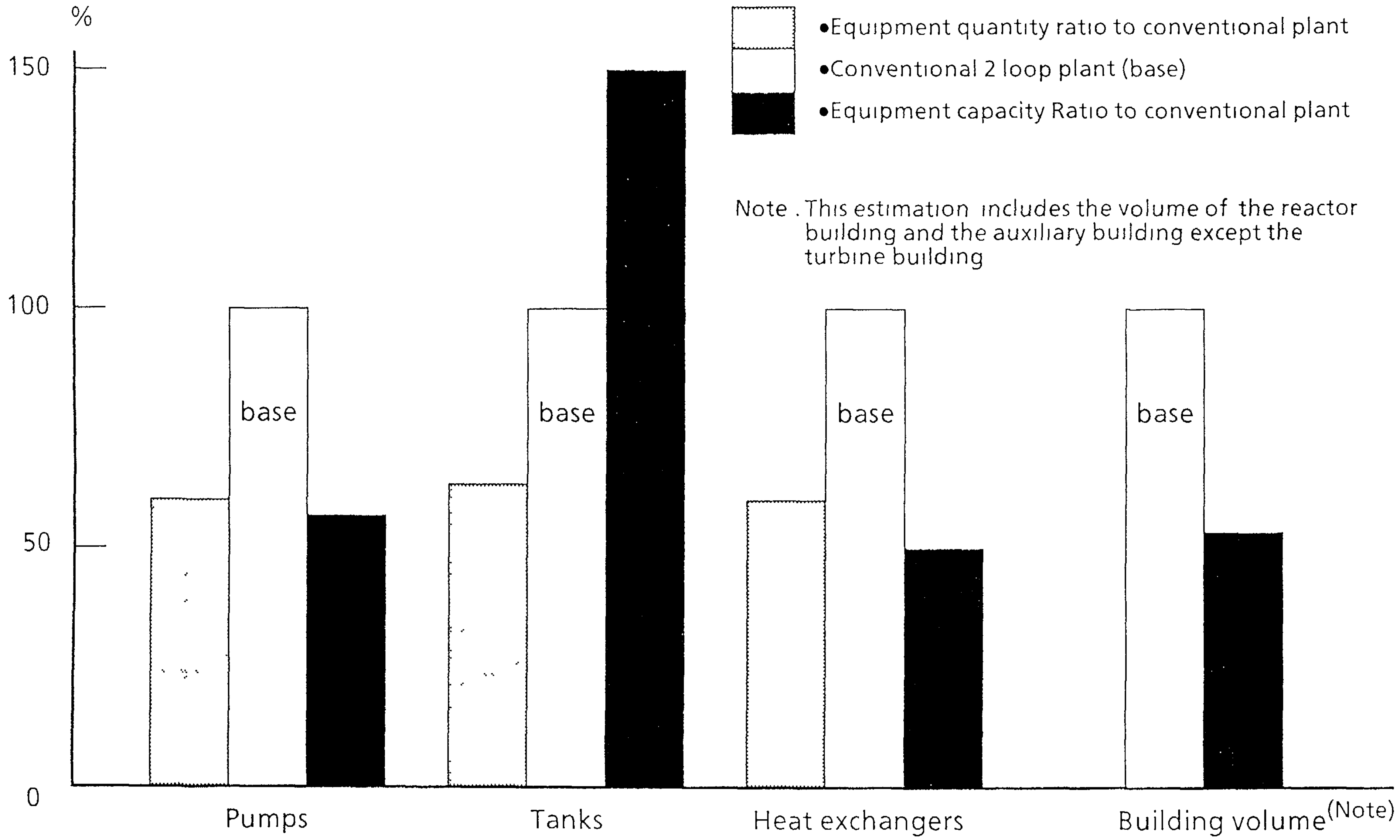
3. Plant design

The MS-600 has a spherical containment vessel with a diameter of 52 meters which provides a good storage capability. The operating floor is at the equator, and the gravity injection pit that also serves as the refueling water storage tank is located on the operating floor. The polar crane is supported from the wall of the pit. Below the operating floor are the RC loops, and the advanced accumulators. Also, the residual heat removal system is located inside the containment vessel so avoiding the possibility of an interface LOCA. Refueling operations are fully automated and the related equipment such as the spent fuel pit is installed inside the containment vessel which results in simpler operations and facilities.

Fig.I-5 describes the results of comparing the main components and material quantities for the 600MWe class plant with those of a typical conventional 2 loop plant. Adoption of the hybrid safety systems has enabled a reduction to be made in the number and capacity of pumps and heat exchangers as well as in the volume of the buildings. The major factors in reducing the quantities are explained below.

* Due to the adoption of hybrid safety systems,

○ The functions for the existing active systems have been reduced, and recirculation system and the C/V internal spray system are no longer needed.



Note . This estimation includes the volume of the reactor building and the auxiliary building except the turbine building

Fig I -5 MS-600 SIMPLIFIED DESIGNING

○ By using steam generators in the passive safety systems, the total heat exchanger capacity could be reduced.

* By installing the SF Pit inside the C/V, the refueling building has been eliminated and the total building volume has been reduced.

However, the total tank capacity has increased as the new system is designed to remove 3 days of decay heat from the reactor core and spent fuel by evaporation of water.

4. Design status

The basic design of the hybrid safety systems has been completed for the 600MWe plant, and several design confirmation tests are being performed. We are also intending to investigate their application to larger capacity plants about 1400MWe.

5. Conclusion

The hybrid safety systems can improve the safety and achieve simplification of a plant to make the systems easier to operate. They use technologies which have already been developed and build on experience which has already been gained from existing plants. By studying the performance of active and passive systems an effective combination can be developed which incorporates the advantages of passive systems as far as possible. We believe that this is the ideal system for the next generation of reactors.

II. Description of key features in 15 design areas

1. Plant process control systems

(1) There are provided the necessary nuclear and process instrumentation required for normal operation and protection action such as neutron flux, temperature, pressure, water level, flow rate and so on. And the reactor control systems are provided in order to automatically control the reactor in case of design load changes.

(2) The reactor control systems are designed as follows.

i. Reactor power is followed by turbine load at normal operation.

ii. The plant is controlled so that main plant and system variables remain within their acceptable ranges and their response becomes stable with enough damping ratio.

iii. The operators are able to monitor the status of the plant conditions and manually control plant if necessary.

(3) The reactor control systems are composed of the following sub-systems.

i. control rods control system
ii. boron concentration control system
iii. pressurizer pressure control system
iv. pressurizer water level control system
v. feed water control system
vi. turbine bypass control system
vii. main steam relief valve control system
viii. rod withdrawal block and turbine run back

(4) When abnormal conditions or troubles occurred at normal operation, operators could monitor automatically the plant variables such as neutron flux, temperature, pressure, radioactivity and so on. And the interlock systems are provided so that errors and mis-operations would not result in reaching to abnormal conditions and accident conditions.

2. Automatic safety systems

(1) Automatic safety systems are provided that would safely shut down the reactor, maintain it in a cooled state and limit any release of fission products, if various anticipated abnormal transients and accidents occurred.

(2) In order to attain above functions, multiple reactor trip signals and engineered safeguards system actuation signals are provided. Engineered safeguards systems include emergency core cooling system, reactor-containment vessel isolation valves, and so on.

Hybrid safety sytems have both of the active safety systems and the passive safety systems. The safety and protection logic for them is investigated to eliminate their adverse interaction. The main operating logic are summarized as follows;

• Reactor trip signal	- Same as a conventional plant (including primary system low pressure 1) - SGTR signal
• Safety injection actuation signal (Active system actuation signal)	- Primary system low pressure 2 (note:the primary depressurization system is not actuated by the safety injection actuation signal)
• Primary depressurization system actuation signal (Passive system actuation signal)	- Primary system low pressure 3 (Combined with main steam pressure higher than low set point) - Safety injection not actuated by the safety injection actuation signal (i.e.active system fails to operate)
• Secondary depressurization system actuation signal	- Primary system low pressure 4 (Combined with primary depressurization system actuated)
• SGTR signal	- Main steam line radiation monitor high

(3) Automatic safety systems are designed to have redundancy and independency and fulfill their safety function, if single failure of system occurred. And they are able to be tested to perform their safety functions during normal operation or refueling shutdown.

3. Protection against power transient accidents

(1) The reactor core is designed so that reactor power could be sufficiently suppressed by its inherent negative reactivity feedback characteristic which consists of Doppler coefficient, moderator temperature coefficient, moderator

void coefficient and so on, if abnormal transients with rapid increase in reactivity occurred at normal operation.

(2) As reactor shutdown systems, there are provided two independent systems which mechanism is different, one is insertion of reactor control rods clusters by reactor control rods control system and another is injection of boric acid by chemical and volume control system.

(3) The reactor control rods clusters are designed so that the reactor could be subcritical at hot condition by insertion of the reactor control rods clusters, if one reactor control rods cluster which has the largest worth was stuck at the fully withdrawal position and not able to be inserted into the reactor core.

(4) The chemical and volume control system is designed so that the reactor could remain sufficiently subcritical at both hot and cold condition including xenon build up condition, by injection of boric acid into the core.

4. Reactor core integrity

(1) The fuel assemblies are designed so that each element of assembly could have enough strength and maintain its mechanical function under both normal operation and anticipated abnormal transient condition. Further they are designed not to affect the function of non fuel bearing components.

(2) Fuel rods are designed to satisfy the following criteria under both normal operation and anticipated abnormal transient condition.

i. Maximum temperature at the center of fuel rod shall be under the melting point of UO_2.

ii. Inner pressure of fuel rod shall not exceed the normal operation pressure of the reactor coolant.

iii. Stress of fuel cladding shall not exceed the proof stress of the cladding material.

iv. Deviation of circumferential tensile strain of fuel cladding shall not exceed 1% in case of each transient

v. Cumulative fatigue cycles shall be within the limit of design fatigue life.

5. Automatic shutdown systems

(1) Safety shutdown systems are fundamentally independent in function from the reactivity control systems used for normal operation. If the signals of the instrumentations from the safe shutdown systems are also used for the plant process control systems, isolation amplifiers are provided at the branch of signals so that troubles such as shortage or break of circuits of the output side (the plant process control systems) would not affect the function of the input side (the safe shutdown systems).

(2) The plant is designed so that the probability of ATWS is sufficiently low and the probability of large amount of fission products release to public is as low as possible.

6. Normal heat removable

(1) The plant is designed so that heat of the reactor is removed by steam generators at normal operation and early phase after reactor shutdown. This steam from the steam generators is either cooled by the turbine condensers or released to the atmosphere through the atmospheric relief valves. After pressure and temperature of reactor coolant become lower than the predetermined value, residual heat removable systems are provided to remove the residual heat of the core.

(2) Residual heat removable systems are designed so that temperature of reactor coolant can be decreased to 60°C within around 20 hours after reactor shutdown, using all trains of the systems.

7. Emergency heat removable

(1) Emergency core cooling systems are designed so that serious damage of fuels and fuel cladding could be protected and reaction between cladding metal and water could be limited to the sufficiently small amount.

(2) Emergency core cooling systems are composed of high head injection systems and auxiliary feed water systems for non-LOCA events, and accumulator injection systems, gravity injection systems, and passive core cooling system with steam generators for LOCA.
High head injection systems and auxiliary feed water systems are designed to automatically start by active system actuation signal and be power-supplied from diesel generators through emergency buses in case of blackout condition. Accumulator injection systems and gravity injection systems are designed to start injection to the core by automatic opening of check valves when pressure of reactor coolant becomes below the operating pressure of accumulators and gravity injection pit. The passive core cooling system is designed so that heat of the core could be transported to the secondary side through the steam generators by natural circulation of reactor coolant, and then water in the secondary side, which is injected from the condensate storage tank by gravity, is evaporated and the steam is released from the secondary side depressurization valves.

(3) Continuous injection to the reactor core and core cooling following a LOCA is confirmed by the analysis. Analysis has been performed assuming a break size equivalent to a 1 inch diameter hole in the vapor space of the pressurizer and also assuming the reactor is tripped and the external power source is lost simultaneously.
Fig.II-1 shows the transients for the primary and secondary system pressure for the case in which the safety injection system fails to operate, and pressure drops to the low pressure signal 3, resulting in the actuation of the depressurization system.
By the time the small flow injection from the accumulators ends, pressure in the primary system has been reduced to a low value so that injection from the gravity injection systems can take over. The constant flow from the pit will keep the core cooled. Even with larger break sizes, the calculated performance of the Emergency Core Cooling System is completely satisfactory. Thus it has been confirmed that the required injection flow and cooling of the reactor core can be achieved by the passive safety systems.

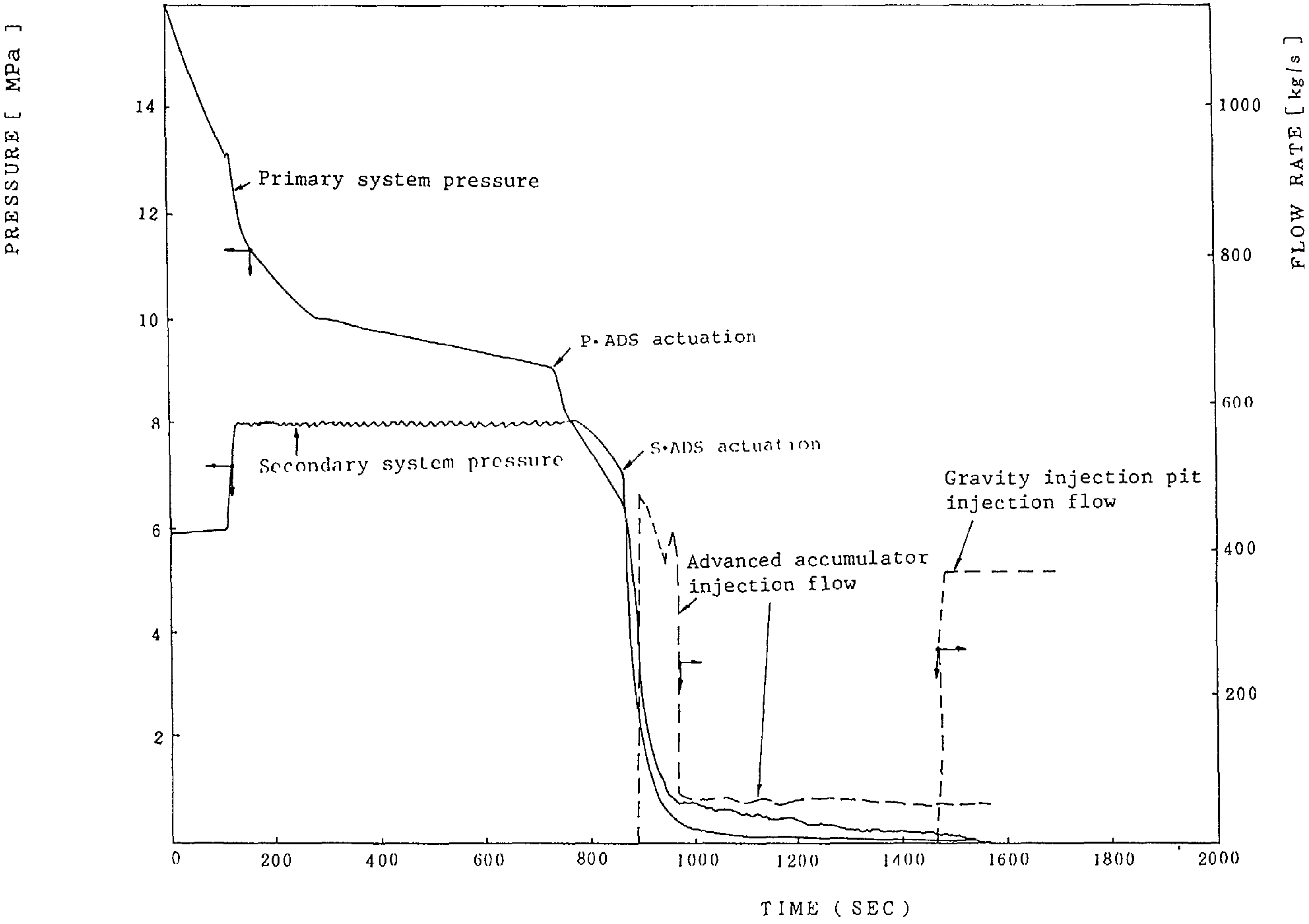


Fig II-1 Pressure and injection flow transient at small-size LOCA (1 inch breakage, SI not working)

(4) Emergency core cooling systems are designed to have independency to be able to attain required safety functions without off site power, even if single failure of the components occurred.
Moreover, the diversity of the safety function is achieved in the hybrid safety systems which are composed of the active safety systems and the passive safety systems.

(5) Emergency core cooling systems are designed so that periodical tests and inspections could be available for each independent system to verify their integrity and redundancy.

8. Reactor coolant system integrity

(1) The reactor coolant pressure boundary is designed taking attention to selection of material, seismic strength, over pressure protection and so on so that the probability of abnormal leakage of reactor coolant and break of pressure boundary would be extremely small. And it is also designed so that inservice inspections could be available to verify its integrity.

(2) The pressure and temperature of the reactor coolant pressure boundary is designed to remain within the limited range at all the anticipated operating conditions by means of primary reactor coolant systems, engineered safeguard systems, reactor auxiliary systems, instrumentation and control systems and so on. The components such as reactor vessel, pressurizer, steam generators are verified to have enough strength by analysis considering each anticipated transient conditions.

(3) Instrumentations such as radiation monitors are provided to quickly detect the leakage of reactor coolant from the reactor coolant pressure boundary. If these instrumentations detected abnormal conditions, operators cold realize the status of the plant by means of annunciators in the control room.

(4) The reactor coolant pressure boundary is designed to avoid brittle characteristic and rapid propagation type of destruction. Therefore, for ferritic steel vessels, careful attention is paid to material, design, fabrication and operation. From the standpoint of preventing brittle failure of components, heat-up and cool-down rate is controlled to be within a limited value and also operating temperature is controlled to be more than pre-determined minimum value for material. For the reactor vessel, surveillance test pieces installed in the reactor vessel are periodically taken out in order to confirm the lowest operable temperature which is increased by the neutron radiation.

(5) The neutron radiation to the MS-600 reactor vessel could be reduced due to newly adopted 40 radial reflector modules made of stainless steel rods which are installed at the core periphery. And a forging ring is used for the core region of the reactor vessel so that weld lines can be deleted in the core region and both integrity and inspectability could be enhanced.

9. Confinement of radioactive material

(1) The peak value of containment internal pressure at a LOCA is kept below the design pressure by the passive safety systems alone, and the internal spray systems are not adopted. Depressurization after 3 days is assumed to be done by using active components.
The calculation of the C/V pressure at a LOCA has also been performed to confirm the accident sequence.

For the purpose of determining the containment vessel pressure, the mass and energy release has also been calculated assuming a double ended break of the primary coolant pipe. The results are shown in Fig.Ⅱ-2

(2) The reactor containment vessel is designed to be capable of conducting leak rate tests to verify that the total leak rate would not exceed the design value. And out of the penetrations, the electrical penetrations, air-locks and so on, are designed to be able to conduct leak test or leak rate test individually or in small groups.

(3) The passive annulus system is provided to reduce radioactivity release to the circumstances at the accidents. The passive annulus system is designed to remove iodine in the gas which leaks from the reactor containment vessel at the accidents.
As show in Fig.Ⅱ-3, the conventional concrete outershield is replaced with a concrete and steel structure in which the concrete fills the space between two steel plates like sandwich. Combined with the steel plate containment vessel, it forms a double containment vessel. This will make the annular space between the containment vessel and outer shield a sealed leak-tight space completely enclosed with steel, so in terms of safety assessment, the radioactive gas which is assumed to leak at the time of accident will be trapped in the annulus.

(4) For the case of the steam generator tube rupture, we have performed analysis to confirm its affect.
In the case of the steam generator tube rupture, the following operations, which are done manually in a conventional plant, are mostly designed to be automatic in the plant with hybrid safety systems.

* Radiation in the main steam is detected by main steam line N-16 monitors, and the reactor trip is done automatically as also is the actuation of the safety injection system and the isolation of the faulty steam generator.

* Temperature and pressure reduction is carried out automatically by using the secondary side depressurization systems small diameter valves located on the secondary side of the intact steam generator. In future studies will be made to see if the turbine bypass valves can be put into operation automatically if an external source of power is available. Auxiliary feedwater supply to the intact steam generator is started automatically.

* Depressurization by automatic actuation of the pressurizer spray (if an external source of power is available the normal spray is used, and if there is no external source of power, a spray supplied from a line branching off the safety injection system is used.)

* Safety injection can be terminated by the operator (30 minutes after the reactor trip to allow time to evaluate safety.)

Stopping the safety injection system will have a direct effect on reactor core cooling, therefore it has been concluded that it would be appropriate for an operator to do this manually after carefully checking the reactor core cooling conditions. In other respect all operations are automated.

Fig.Ⅱ-4 shows analysis results for the pressure transients of the primary and secondary systems for the case of a double ended break of a steam

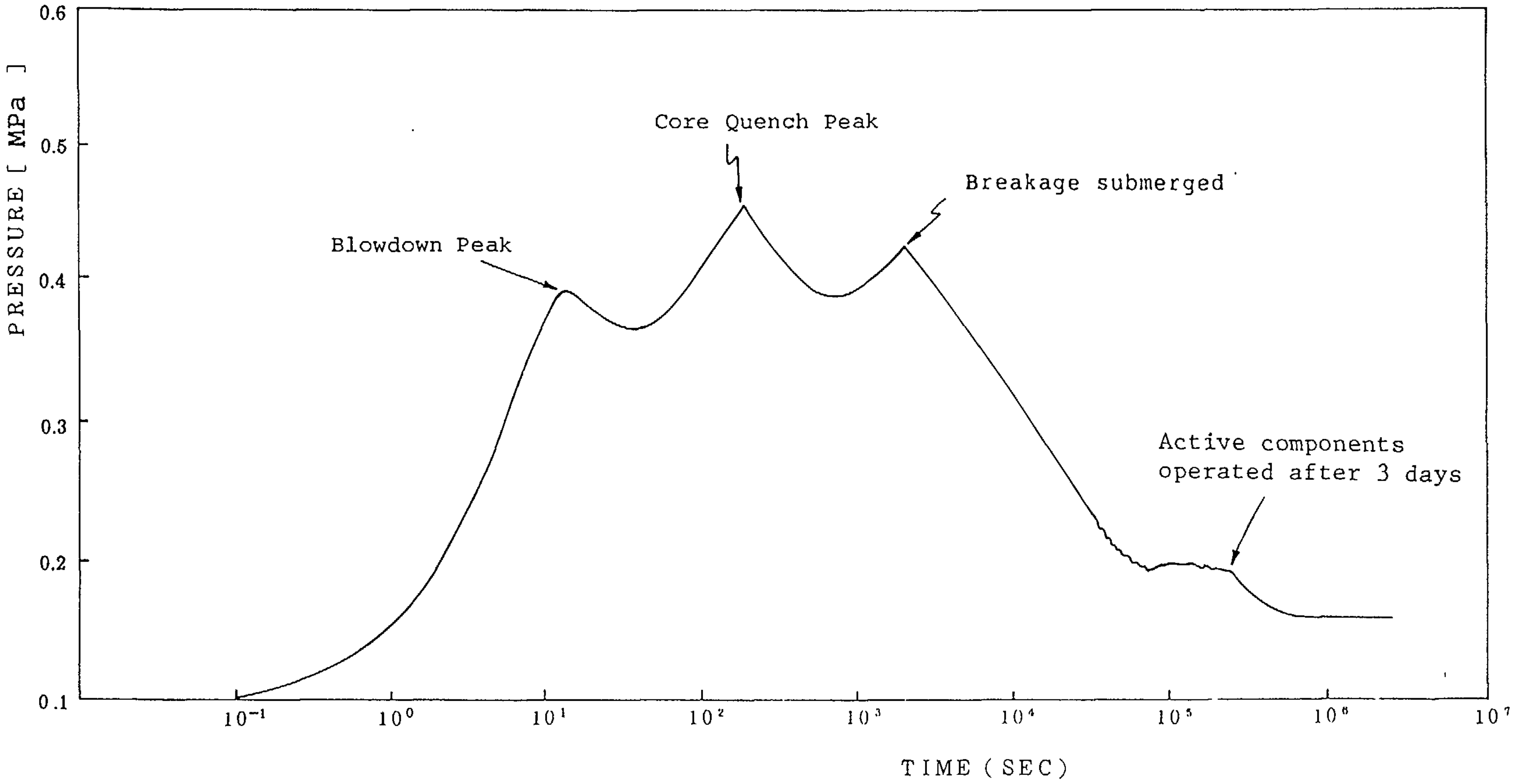
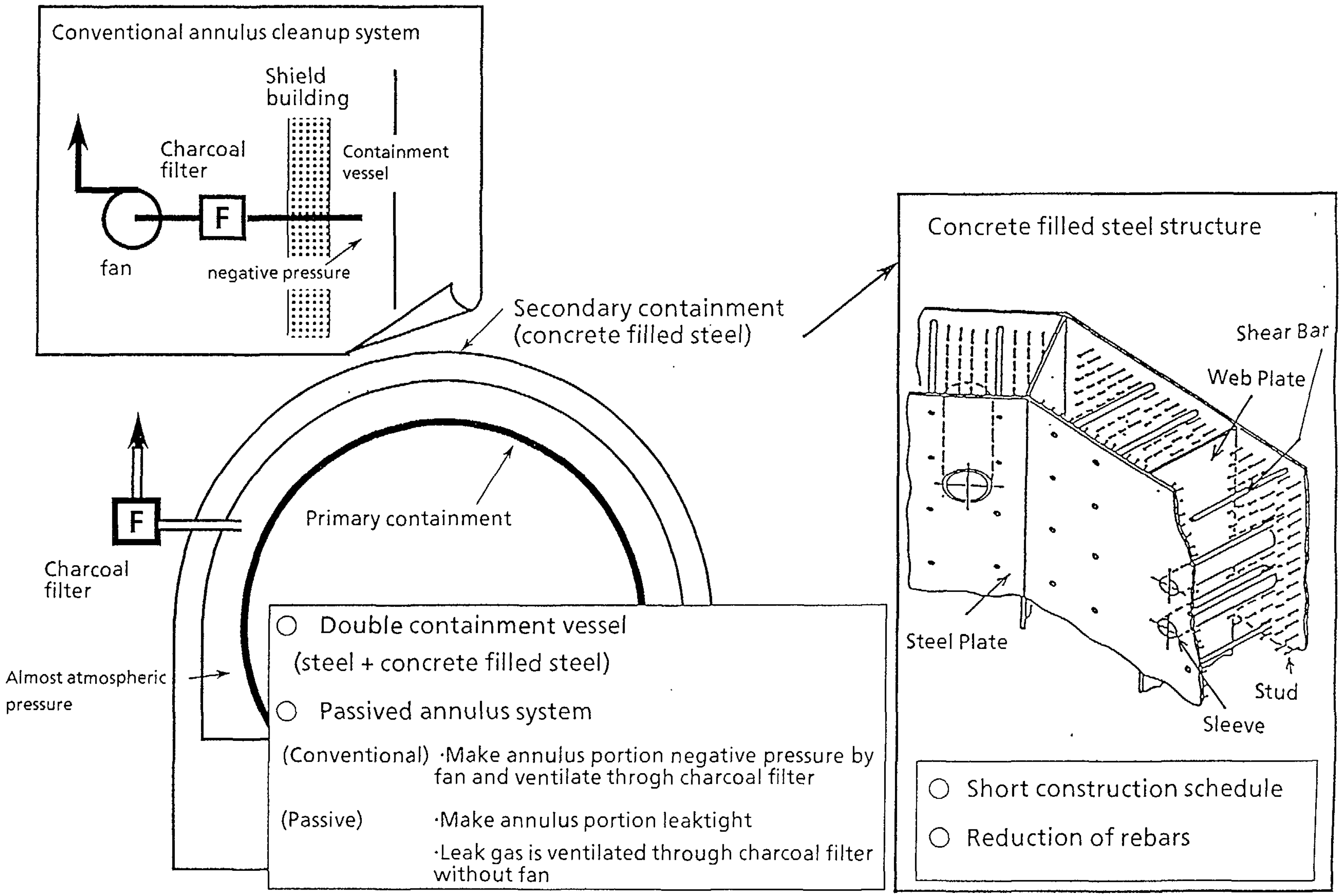


Fig II-2 Containment pressure transient at large-size LOCA



○ Double containment vessel
(steel + concrete filled steel)

○ Passived annulus system

(Conventional) ·Make annulus portion negative pressure by fan and ventilate throgh charcoal filter

(Passive) ·Make annulus portion leaktight
·Leak gas is ventilated through charcoal filter without fan

○ Short construction schedule

○ Reduction of rebars

Fig II -3 Passive annulus filter system by using double containment

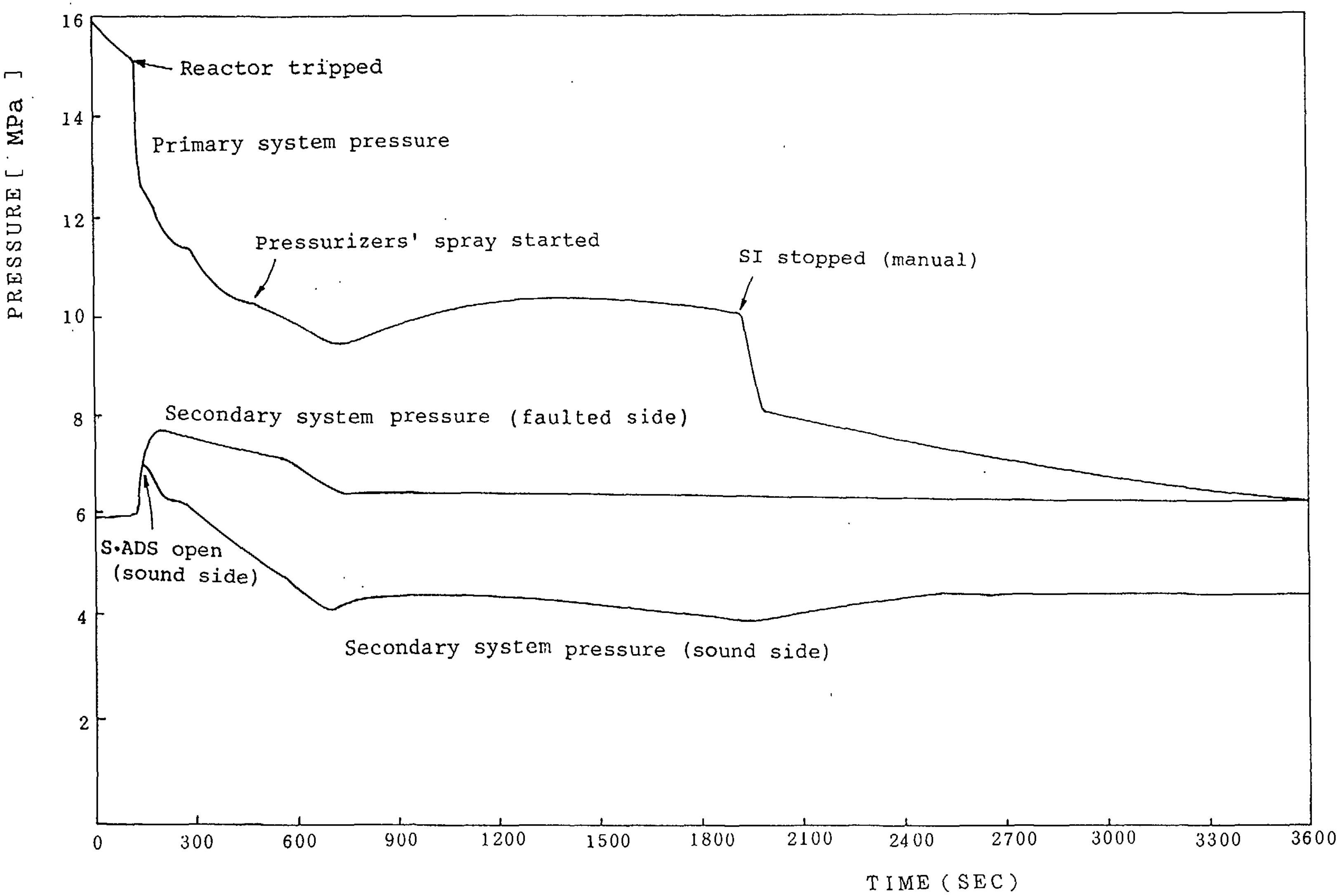


Fig II-4 Analysis result for SGTR (with external power source)

generator tube, with external power available. Due to early isolation of the faulty steam generator and heat removal, the relief valves of the secondary side of the faulty steam generator are not actuated, and there is no direct release of contaminated steam to the air. The amount of primary coolant passing through the break to the secondary system is less than that of a conventional plant.

Also, if the automatic safety injection does not take place or if, on the contrary, the injection continues for too long and the water level in the gravity injection pit drops to an abnormally low level then the depressurization system is automatically actuated, as an additional safety measure.

10. Protection of confinement structure

(1) The plant is designed to reduce the probability of occurrences of severe core accidents to the extremely low level. Therefore, severe core accidents are not considered to be design basis accidents.

(2) Study on improvement of the mechanical integrity of the reactor containment vessel and several mitigation measures at the severe core accidents is on going.

11. Monitoring of plant safety status

(1) Various kinds of plant variables required for operation at the accidents are designed to be monitored in the control room. It is important to detect rapidly the abnormal condition, because operator action in the early phase of the accidents might protect the expansion of the abnormal conditions to the accidents. From this point of view, loose parts monitors, vibration / noise monitors, leak detectors, radiation monitors, thermometers and so on are provided to be monitored in the control room.

(2) From the view point of enhancing man-machine interface, the main control panels are designed to be console type and be capable of monitoring and operating only on the screen of CRTs, so-called touch screen type. Adopting such design could supply selected plant variables in an intensive manner to the operators at the accidents.

12. Preservation of control capability

(1) Cables and control panels are designed to be made of noninflammable or almost noninflammable material as far as practical, so that the probability of occurrence of fires in the control room would be extremely low.

(2) The control room is designed so that the operators could remain there and conduct necessary actions, if the accidents occurred, by means of the provisions of the appropriate shield and the heating and ventilation systems.

(3) If the operators could not remain in the control room for any reason, the plant is designed so that the operators could shutdown the reactor safely. The operators could shutdown the reactor rapidly by means of either opening the reactor trip breakers in the control rod drive mechanism electrical power panel room, or tripping the turbine at remote location. Further, and alternative panel somewhere outside the control room is provided so that the operator actions could be taken for the components which are often used for the hot standby operation or are used for the short period after the reactor trip and minimum plant variables required for this operator action could be available.

13. Station blackout

(1) As electrical power supply to the station, in addition to the off-site power strongly connected to the grids, there are provided two trains of emergency diesel generator systems which supply power to the emergency busses. Therefore, the probability of loss of electrical power supply even in the limited period would be extremely low. However, if short time station black out occurred, the reactor could be safely shut down by means of the actuation of the reactor safe shutdown systems. Further, heat removable of the core could be attained by means of both natural convection of the reactor coolant in the primary side and actuation of the turbine driven auxiliary feed water pumps and main steam safety valves in the secondary side. Electrical source of the reactor safe shutdown systems and the turbine driven auxiliary feed water systems would be supplied from the highly reliable battery.

14. Control of accidents within the design basis

(1) There are provided the plant control systems and automatic safety systems so that the plant could be returned to the normal condition if abnormal conditions occurred, and the reactor could be shut down and large release of fission products could be protected if the accidents occurred. And the operating procedures required for the above abnormal and accidental conditions are clarified and reflected into the plant design.

(2) If manual operations were required, the plant is designed so that more than 30 minutes would be available for the operators to realize the plant status precisely and to be confident of that the operator manual action would not affect the control of the abnormal conditions and accidents.

(3) Core damage frequency of small LOCA, which is one of dominant initiating event to core damage in conventional plants, was calculated via reliability evaluation of the event heading in Fig.Ⅱ-5.

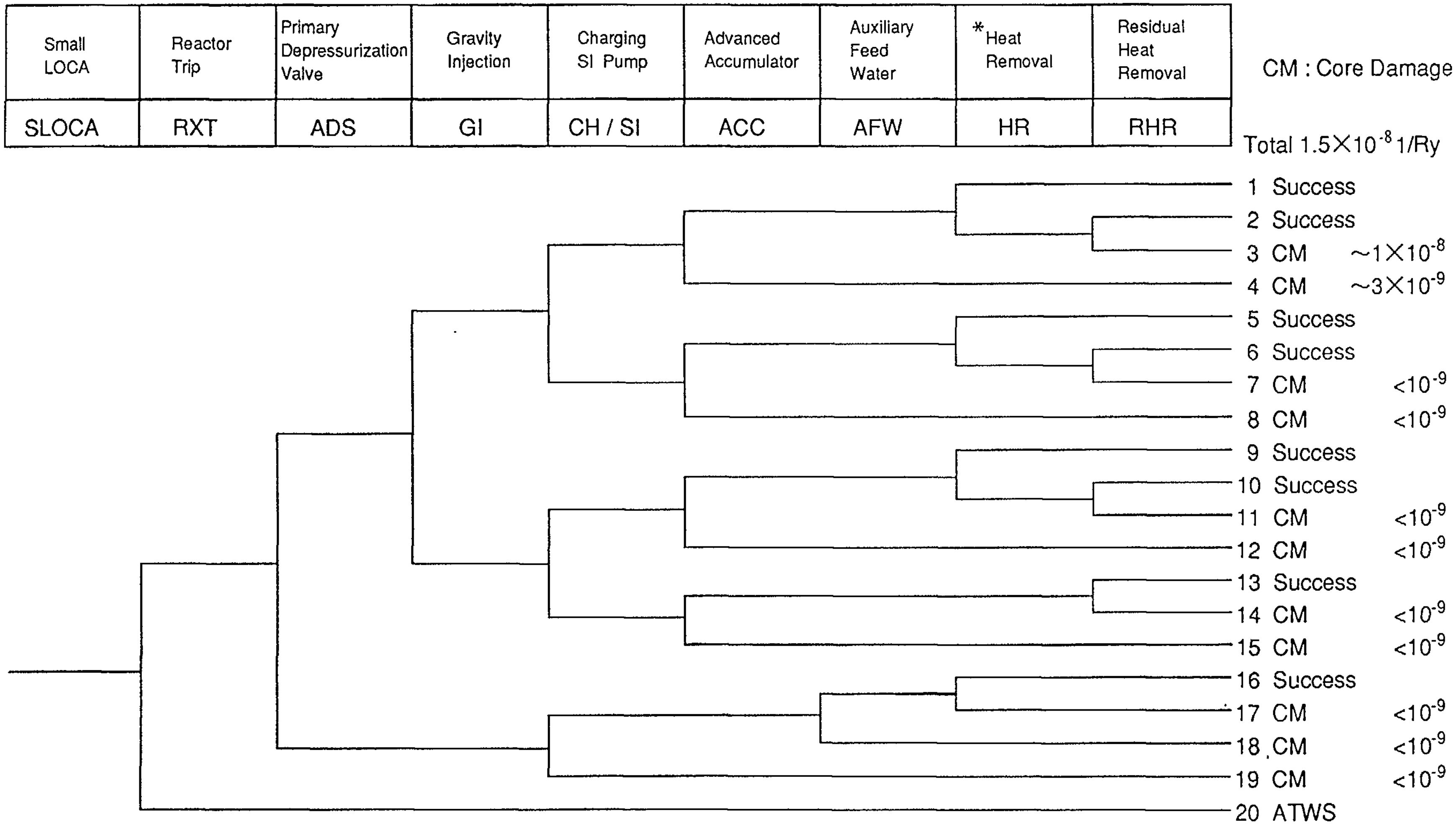
The core damage frequency of the hybrid safety system plant is one order magnitude less than of the conventional plant. This result indicates that the hybrid safety systems improve safety.

It has also confirmed that the plant safety could be further improved by improving the reliability of the secondary side depressurization system, the secondary gravity injection system, and the primary side gas vent system.

15. Mitigation and control of severe accidents

(1) The plant is designed to reduce the probability of occurrences of severe core accidents to the extremely low level. Therefore, severe core accidents are not considered to be design basis accidents.

(2) Study on improvement of the mechanical integrity of the reactor containment vessel and several mitigation measures at the severe core accidents is on going.



*SADS (Secondary Depressurization Valve)
Feed Water
Primary System Gas Vent

Fig II-5 Small LOCA Event Tree

III. List of main parameters

MS-600 PRINCIPAL PARAMETERS

PARAMETERS	MS-600	PARAMETERS	MS-600
Electrical output (MWe)	~630	Reactor coolant system	
		Number of loops	2
NSSS thermal output (MWt)	1825	Operating pressure (MPa)	15.4
Reactor type	PWR	Temperature	
		Reactor outlet (°C)	325.0
Rector core	15.1kW/m (Low power density core)	Reactor inlet (°C)	290.6
		Steam generators	
Fuel assemblies		Number	2
Type	17 × 17	Type	Horizontal, U-Tube type
Number	145		
Turbine	TC4F40	Steam pressure (MPa)	5.7
	Hybrid safety systems	Reactor coolant pumps	
Safety system		Number	2
		Type	High efficiency type with improved seals

Next page(s) left blank

Appendix II
LIST OF PARTICIPANTS

LIST OF PARTICIPANTS

Antonovski, G.
OKB Mechanical Engineering
Burnakovsky proezd 13
603603 Nizhny Novgorod 74
Russian Federation

Bakhmetyev, A.
OKB Mechanical Engineering
Burnakovsky proezd 13
603603 Nizhny Novgorod 74
Russian Federation

Bandurski, T.
Department 412
Paul Scherrer Institute (Area East)
CH-5232 Villigen PSI
Switzerland

Bartlett, J.
Nuclear Installations Inspectorate
Nuclear Safety Division
St. Peters House, Stanley Precinct
Bootle, Merseyside
L2O 3LZ United Kingdom

Berger, J.-P.
EdF - Construction and Engineering Division
12 avenue Dutrievoz
69628 Villeurbanne, France

Berkovitch, V.
PI "Atomenergoprojekt"
Bakuninskaya st. 7/1
107817 Moscow
Russian Federation

Birykov, G.
OKB "Gidropress"
Ordjinikidze st. 21
142103 Podolsk, Moscow District
Russian Federation

Czech, J.
Siemens AG, Power Generation (KWU)
Department NA-T
P.O. Box 3220, Koldestr. 16
D-91050 Erlangen, Germany

Dennielou, Y.
Electricité de France/Septen
SCE études et projets thermiques et nucléaires
12-14 avenue Dutrievoz
F-69628 Villeurbanne Cedex
France

Fagerholm, R.
Division of Concepts and Planning
Department of Safeguards
IAEA, Wagramerstrasse -5
P.O. Box 100
A-1400 Vienna, Austria

Gagarinski, A.
RRC "Kurchatov Institute"
Kurchatov squ. 1
123182 Moscow
Russian Federation

Gherardi, G.
ENEA Departement de l'Energie
Via Martiri di Monte Sole - 4
40129 Bologna, Italy

Goetzmann, C.A.
(Scientific Secretary)
IAEA, Division of Nuclear Power
Wagramerstrasse - 5
P.O. Box 100
A-1400 Vienna, Austria

Ignatyev, V.
RRC "Kurchatov Institute"
Kurchatov squ. 1
123182 Moscow
Russian Federation

Kukardin, E.
Ministry of Science and Technical Politic
of Russian Federation
Tverskaya st. 9
103905 Moscow
Russian Federation

Kukharkin, N.
RRC "Kurchatov Institute"
Kurchatov squ. 1
123182 Moscow
Russian Federation

Kupitz, J.
Division of Nuclear Power
International Atomic Energy Agency
Wagramerstrasse - 5
P.O. Box 100
A-1400 Vienna, Austria

Krett, V.
(Scientific Secretary)
Nuclear Power Technology Development Section
Division of Nuclear Power
International Atomic Energy Agency
P.O. Box 100
A-1400 Vienna, Austria

Kuul, V.

OKB Mechanical Engineering
Burnakovsky proezd 15
603603 Nizhny Novgorod 74
Russian Federation

Lang, P.

Office of Nuclear Energy
U.S. Department of Energy
Mail Stop NE-451
Washington, D.C. 20585, USA

Meyer, P.-J.

Siemens AG, Group KWU, N Ref SM
Nuclear Power Generation
Strategy and Marketing, International
Organizations, Export Licensing
P.O. Box 3220
D-91050 Erlangen, Germany

Mink, E.

Westinghouse
Energy Systems International
Rue de Stalle 73
1180 Brussels
Belgium

Novikov, V.

RRC "Kurchatov Institute"
Kurchatov squ. 1
123182 Moscow
Russian Federation

Pedersen, T.

Safety and Operation
Nuclear Systems Division
ABB Atom AB
S-72163 Västerås, Sweden

Ponomarev-Stepnoi, N.

RRC "Kurchatov Institute"
Kurchatov squ. 1
123182 Moscow
Russian Federation

Ritterbusch, S.E.

Standard Plant Licensing
ABB Combustion Engineering
1000 Prospect Hill Road
Windsor, CT, USA 06095

Teske, H.

Gesellschaft für Anlagen- und
Reaktorsicherheit (GRS) mbH
Pechotnaja 32-1
123436 Moscow
Russian Federation

Tomanek, P.
State Office for Nuclear Safety
Dr. Bureste 1
Ceske Budejovice
Czech Republic

Volkov, B.
OKB "Gidropress",
Ordjinikidze st. 21
142103 Podolsk, Moscow District
Russian Federation

Voznesenski, V.
RRC "Kurchatov Institute"
Kurchatov squ. 1
123182 Moscow
Russian Federation

Yershov, V.
OKB "Gidropress"
Ordjinikidze st. 21
142103 Podolsk, Moscow District
Russian Federation

Yvon, M.E.
Safety and Licensing
NPI (Nuclear Power International)
6, cours Michelet
92064 Paris la Defense
France