Safety Reports Series
No. 23

# Accident Analysis for Nuclear Power Plants

International Atomic Energy Agency, Vienna, 2002

# IAEA SAFETY RELATED PUBLICATIONS

## IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities.

The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides.**

**Safety Fundamentals** (blue lettering) present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

**Safety Requirements** (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.

**Safety Guides** (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA.

Information on the IAEA's safety standards programme (including editions in languages other than English) is available at the IAEA Internet site

www.iaea.org/ns/coordinet

or on request to the Safety Co-ordination Section, IAEA, P.O. Box 100, A-1400 Vienna, Austria.

## OTHER SAFETY RELATED PUBLICATIONS

Under the terms of Articles III and VIII.C of its Statute, the IAEA makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued in other series, in particular the **IAEA Safety Reports Series**, as informational publications. Safety Reports may describe good practices and give practical examples and detailed methods that can be used to meet safety requirements. They do not establish requirements or make recommendations.

Other IAEA series that include safety related publications are the **Technical Reports Series,** the **Radiological Assessment Reports Series,** the **INSAG Series, the TECDOC Series**, the **Provisional Safety Standards Series**, the **Training Course Series,** the **IAEA Services Series** and the **Computer Manual Series**, and **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**. The IAEA also issues reports on radiological accidents and other special publications.

# ACCIDENT ANALYSIS
# FOR
# NUCLEAR POWER PLANTS

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BANGLADESH
BELARUS
BELGIUM
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHILE
CHINA
COLOMBIA
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
LATVIA
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITIUS
MEXICO
MONACO
MONGOLIA
MOROCCO
MYANMAR
NAMIBIA
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
PAKISTAN
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIET NAM
YEMEN
YUGOSLAVIA, FEDERAL REPUBLIC OF
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world''.



Printed by the IAEA in Austria
November 2002
STI/PUB/1131

SAFETY REPORTS SERIES No. 23

# ACCIDENT ANALYSIS FOR NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2002

**VIC Library Cataloguing in Publication Data**

Accident analysis for nuclear power plants. — Vienna : International Atomic Energy Agency, 2002.
p. ; 24 cm. — (Safety reports series, ISSN 1020–6450 ; no. 23)
STI/PUB/1131
ISBN 92–0–115602–2
Includes bibliographical references.

1. Nuclear power plants—Accidents. I. International Atomic Energy Agency. II. Series.

VICL 02–00299

# FOREWORD

Deterministic safety analysis (frequently referred to as accident analysis) is an important tool for confirming the adequacy and efficiency of provisions within the defence in depth concept for the safety of nuclear power plants (NPPs). Owing to the close interrelation between accident analysis and safety, an analysis that lacks consistency, is incomplete or is of poor quality is considered a safety issue for a given NPP. Developing IAEA guidance documents for accident analysis is thus an important step towards resolving this issue.

Requirements and guidelines pertaining to the scope and content of accident analysis have, in the past, been partially described in various IAEA documents. Several guidelines relevant to WWER and RBMK type reactors have been developed within the IAEA's Extrabudgetary Programme on the Safety of WWER and RBMK NPPs. To a certain extent, accident analysis is also covered in several documents of the revised NUSS series, for example, in the Safety Requirements on Safety of Nuclear Power Plants: Design (NS-R-1) and in the Safety Guide on Safety Assessment and Verification for Nuclear Power Plants (NS-G-1.2). Consistent with these documents, the IAEA has developed the present Safety Report on Accident Analysis for Nuclear Power Plants. Many experts have contributed to the development of this Safety Report. Besides several consultants meetings, comments were collected from more than fifty selected organizations. The report was also reviewed at the IAEA Technical Committee Meeting on Accident Analysis held in Vienna from 30 August to 3 September 1999.

The present IAEA Safety Report is aimed at providing practical guidance for performing accident analyses. The guidance is based on present good practice worldwide. The report covers all the steps required to perform accident analyses, i.e. selection of initiating events and acceptance criteria, selection of computer codes and modelling assumptions, preparation of input data and presentation of the calculation results. This safety report also discusses various factors that need to be considered to ensure that the accident analysis is of an acceptable quality.

The report is intended for use primarily by analyses co-ordinating, performing or reviewing accident analyses for NPPs, on both the utility and regulatory sides. The report will also be of use as a background document for relevant IAEA activities, such as training courses and workshops. While the main body of the report does not focus exclusively on a single reactor type, the examples provided in the annexes are related mostly to the accident analysis of NPPs with pressurized water reactors. The report:

- Applies to both NPPs being built and operating plants;
- Deals with internal events in reactors or in their associated process systems; thus the emphasis is on the physical transient behaviour of reactors and their systems, including reactor containment;

- Discusses both best estimate and conservative accident analyses;
- Covers design basis accidents as well as beyond design basis accidents, although the design basis accidents are covered in greater detail;
- Focuses on thermohydraulic aspects of safety analysis; neutronic, structural and radiological aspects are also covered to some extent;
- Covers the course of an accident from the initiating event up to source term estimation.

The main body of the report is intended to be as generally applicable as possible to all reactor types.

The IAEA staff member responsible for this publication was J. Mišák of the Division of Nuclear Installation Safety.

# CONTENTS

# 1. INTRODUCTION

## 1.1. BACKGROUND

The safety of nuclear power plants (NPPs) is based on the defence in depth concept, which relies on successive physical barriers (fuel matrix, cladding, primary system pressure boundary and containment) and other provisions to control radioactive materials and on multiple levels of protection against damage to these barriers and against undue radiological impact on the NPP itself and on its surroundings. Demonstration that there is no undue risk caused by plant operation is obtained by means of safety assessment of an NPP. Further details on the defence in depth concept and on safety assessment can be found in Refs [1–5].

As explained in Ref. [3], safety assessment is a broad term describing a systematic process aimed at ensuring that all relevant safety requirements are met, including: the principal requirements (e.g. sufficient defence in depth, accounting for the operating experience and safety research), plant equipment requirements (e.g. equipment qualification and consideration of the ageing and reliability of systems through redundancy and diversity) and plant systems design requirements (e.g. specific requirements on the reactor core, reactor coolant system, containment and engineered safety features). More generally, safety assessment can cover all aspects of the siting, design, construction, operation and decommissioning of an NPP that are relevant to safety.

Safety assessment includes safety analysis as an essential component, but is not limited to it. By the term safety analysis an analytical study is meant by which it is demonstrated how safety requirements, such as ensuring the integrity of barriers against radioactive releases and various other requirements, are met for initiating events (both internal and external) occurring in a broad range of operating conditions, and in other circumstances, such as varying availability of the plant systems. Two properly balanced complementary methods of safety analysis, deterministic and probabilistic, are used jointly in evaluating the safety of an NPP.

The entire range of conditions for which an NPP is designed according to established design criteria, including all the national regulatory requirements, and for which damage to the fuel and release of radioactive material are kept within authorized limits, form the design basis of an NPP. Within the design basis, a number of unintended events are considered, including operating errors and equipment failures, whose consequences or potential consequences are not negligible in terms of safety. According to the probability of its occurrence and potential consequences, an event may be classified as an anticipated operational occurrence (also called a transient) or a design basis accident (DBA).

An accident occurring outside the NPP design basis is called a beyond design basis accident (BDBA). Such an accident may or may not involve degradation of the reactor core (leading to significant core damage). An accident involving core degradation (typically with core melting) is also called a severe accident. According to the IAEA Safety Requirements on the Safety of Nuclear Power Plants: Design [1], in paragraph 5.31, severe accidents are also to be considered in the design and operation of NPPs, and some regulatory bodies prescribe that these accidents be taken into consideration in the plant design.

Deterministic safety analysis predicts the response of an NPP in specific predetermined operational states to postulated initiating events. This type of safety analysis applies a specific set of rules and specific acceptance criteria. Deterministic analysis is typically focused on neutronic, thermohydraulic, radiological and structural aspects, which are often analysed with different computational tools.

Probabilistic safety analysis (PSA) combines the likelihood of an initiating event, potential scenarios in the development of the event and its consequences into an estimation of core damage frequency, source term or overall risk arising from operation of the NPP. The number of event sequences can be very large.

There may be a broad variation in the assumptions used in the deterministic safety analysis. The physical models themselves (as implemented in the computer codes) may be intended to be realistic (‘best estimate’) or may be deliberately biased in a pessimistic manner. Likewise the input data and assumptions may be design and/or operational values (realistic) or pessimistic values (conservative). Typical combinations are conservative models with conservative data, best estimate models with conservative data and best estimate models with best estimate data. The last combination is called a best estimate analysis and is usually combined with an uncertainty analysis.

Deterministic safety analysis is usually performed through the calculation of plant parameters with complex computer codes, solving a set of mathematical equations describing a physical model of the plant. Confidence in the results, and consequently in the safe design as well as safe operation of the plant, depends strongly on the capability to model related physical phenomena and validation of that capability through relevant experimental programmes and/or real plant operational data (on startup tests, steady state parameters and operational events). The term ‘accident analysis’ is used in this Safety Report to describe deterministic safety analysis of anticipated operational occurrences (transients), DBAs and BDBAs.

Accident analysis is an important tool for confirming the adequacy and efficiency of the provisions in the defence in depth concept to cope with challenges to plant safety. It is used in a number of applications, such as: licensing of new plants; modification of existing plants; periodic safety reviews; analysis of operational events; the development, improvement or justification of the plant operational limits

and conditions; support for emergency operating procedures; operator training programmes; probabilistic studies; development of accident management programmes; and emergency planning.

Requirements and guidelines for the scope and content of accident analysis have been established in several IAEA Safety Requirements [1, 2] and Safety Guides [3, 4]. In addition, several guidelines relevant to (Soviet) water cooled, water moderated, energy reactor (WWER) type reactors have been produced within the framework of the IAEA Extrabudgetary Programme on the Safety of WWER and RBMK NPPs, namely general guidelines [5] and guidelines for pressurized thermal shock analysis [6], for anticipated transients without scram [7], for containment evaluation [8], for the analysis of accidents in shutdown operational modes of WWER NPPs [9] and for the analysis of leaks from the primary to the secondary system [10]. More detailed national standards on performing accident analysis have also been developed in several countries. These standards, namely those from the United States of America [11, 12], Canada [13], the Russian Federation [14, 15], France [16], Germany [17] and Finland [18], have been considered, when appropriate, in this Safety Report. No comprehensive guidance on accident analysis has been issued by the IAEA.

## 1.2. OBJECTIVE

Owing to the close interrelation of accident analysis and ensuring the safety of NPPs, a lack of consistency, completeness or quality in an accident analysis is considered a safety issue for the specific NPP. This Safety Report contributes to eliminating or reducing the safety significance of such issues. It deals mainly with deterministic safety analysis (accident analysis), although aspects of accident analysis in support of probabilistic assessment are also mentioned.

The objective of this Safety Report is to establish a set of suggested methods and practices, conceptual as well as formal, based on current good practices around the world, for performing accident analysis. The Safety Report covers all steps in performing analyses, i.e. the selection of initiating events and acceptance criteria, selection of computer codes and modelling assumptions, preparation of input data and presentation of the results of calculations. Various aspects in ensuring an adequate quality of accident analysis are also discussed in this Safety Report.

Many assumptions made in accident analyses are related to specific national requirements, computer codes and reactor designs. It was therefore not considered appropriate to provide guidance that is too specific and it was intended to maintain an appropriate balance between general and specific suggestions. The information is intended to be used primarily by code users performing accident analysis. Regulatory bodies are encouraged to use the Safety Report in the formulation of national

requirements. This Safety Report may also be utilized by analysts in contacts with their national regulatory body or in the formulation of detailed company procedures.

## 1.3. SCOPE

This Safety Report is applicable to countries with a developing nuclear energy sector and with a regulatory body open to adopting changes to the present set of rules for accident analysis.

The main text of this Safety Report is not focused exclusively on one reactor type, although it is most applicable to accident analysis for NPPs with pressurized water reactors. Although not fully excluded, non-water-cooled reactors, fast reactors, research reactors and other nuclear facilities are not specifically dealt with. This Safety Report is generally applicable to both NPPs under construction and operating plants. The details of its application are subject to approval by the regulatory body.

This Safety Report deals only with 'internal' events originating in the reactor or in its associated process systems. It excludes events affecting broad areas of the plant, such as fires, floods (internal and external) and earthquakes, and also local external events such as aircraft crashes. Thus the emphasis in this guidance is on the physical transient behaviour of the reactor and its systems, including the reactor containment. To some extent, spent fuel pools are also covered owing to their similarities with process systems.

This Safety Report deals with both best estimate and conservative accident analyses. Although most plants were licensed using a fully conservative approach (conservative code and conservative data), such an approach can be misleading in a number of applications, for example, for the development of operating procedures or for probabilistic safety assessment. Thus the use of best estimate computer codes is encouraged. If conservative results are necessary, these can be achieved with either: (a) conservative assumptions on key input parameters and sensitivity analysis to confirm that there is no abrupt change in safety as a parameter changes or (b) an uncertainty analysis, to include the range of consequences for safety in a more rigorous manner.

The methods of accident analysis have been developed significantly over the past two decades from the point of view of a better understanding of physical phenomena, the sophistication of the computer codes and computing capabilities, and the integration of research results into code development and application. This development has made it possible to switch over from the simplified codes to highly sophisticated integral (system) codes. As a result of the development of computer techniques, there are no major limitations in terms of the cost of computer time. For the purposes of this Safety Report, the assumption is made that advanced codes capable of performing a best estimate analysis are generally available.

This Safety Report covers BDBAs as well as DBAs, although DBAs are covered in more detail.

The Safety Report focuses on thermohydraulic aspects of safety analysis. Neutronic and radiological aspects are also covered to some extent. Less consideration is given to structural (mechanical) aspects.

The course of an accident is covered from an initiating event up to a source term estimation. Transport of radioactive materials outside the reactor building is not covered in the main text.

The main text of this Safety Report is intended to be as generally applicable as possible to all reactor types.

## 1.4. STRUCTURE

Sections 2, 3 and 4 of this Safety Report are primarily explanatory. They introduce basic terminology and explain the function of accident analysis in ensuring plant safety. The following sections, although containing some explanatory material, include practical suggestions for users.

Section 2 deals with the proper selection and categorization of initiating events. The relationship to a potential degradation of the safety functions is specified. Several possibilities for grouping events into categories are given and the concept of a bounding accident scenario is introduced. In Section 3, the acceptance criteria for accident analysis are explained and some examples of high level acceptance criteria, derived from the need to maintain fundamental safety functions, are given. Section 4 summarizes the principles of the two basic approaches in performing accident analysis: the conservative approach and the best estimate approach. Suggestions on the proper selection of an approach or a combination of approaches are given.

Section 5 discusses possible applications of analysis including design, licensing, support of emergency operating procedures (EOPs), simulators, PSA, accident management, emergency planning, analysis of operational events and regulatory audit analysis. The main characteristics of each application are presented. Section 6 discusses various issues relating to the application of computer codes for accident analysis. The basic types of features of the codes are described. Comments are given on the documentation of the codes, its verification and validation, and its accuracy, including suggestions on the adequate selection of codes.

Some aspects of the effects of the user on the analysis are discussed in Section 7. The importance of user qualification is discussed with suggestions on how users can be qualified. Additional suggestions for code developers and user organizations for the reduction of user effects are also provided. Section 8 deals with the preparation of input data, including the collection of data from reliable sources, the creation of an engineering handbook and input decks, and checking of the quality of the input data.

Section 9 provides basic rules for the formatting and structuring of results, as well as for reviewing them. Section 10 discusses the importance of quality assurance for accident analysis and summarizes good practices in quality assurance.

There are four annexes, providing more examples for application. Annex I specifies and characterizes the main steps in performing accident analysis. Annex II provides more discussion on, and examples of, uncertainty analysis. Annex III gives a practical example of the preparation of input data for analysis and on the production of the corresponding documents. Annex IV contains references to the typical computer codes for accident analysis.

# 2. CLASSIFICATION OF INITIATING EVENTS

## 2.1. FUNDAMENTAL SAFETY FUNCTIONS

The basic objective for nuclear safety is the protection of individuals, society and the environment from harm by the establishment and maintenance of effective defences against radiological hazards in nuclear installations [19].

To achieve the basic nuclear safety objective in operational states, DBAs and, to the extent practicable, BDBAs, the following fundamental safety functions have to be performed: control of reactivity, removal of heat from the fuel, confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases.

Control of reactivity generally means all the measures taken to avoid inadvertent nuclear criticality, loss of reactivity control, inadvertent power excursions or reduction in shutdown margin. Loss of reactivity control could lead to excessive heat production in the nuclear fuel and to potential damage to the barriers against radioactive releases.

Removal of heat from the nuclear fuel (representing the main source of radioactive material) necessitates that sufficient cooling of the fuel be ensured under all conditions to prevent excessive heating up resulting in a large radioactive release. All potential locations for fuel (the core and the spent fuel pool) and all operational conditions (normal operation at power, shutdown modes and accidents) need to be considered. Performing this fundamental safety function typically necessitates maintaining the integrity of the coolant system, the circulation of coolant and the control of the coolant inventory, and the availability of a heat sink.

Confinement of the radioactive material, both in normal operation and under accident conditions, necessitates that relevant barriers (fuel matrix, cladding, primary system pressure boundary and containment) remain intact or that their degradation be

limited. For some accidents, such as loss of coolant accidents (LOCAs), there is a potential for consequential damage of several barriers. Barriers can be affected by loss of mechanical properties due to excessive heat-up, by overpressurization of the coolant system or the containment, by structural damage due to mechanical impact or jet forces, by thermal fatigue or by fracture propagation, for example.

Once a release of radioactive material is foreseen, either as a routine part of normal operation or as the consequence of an accident sequence, this release will be controlled for the normal operation case and limited or delayed, as much as possible, for the accident condition case.

Incidents or accidents may therefore be initiated whenever a failure, malfunction or faulty operation of a system or component endangers the fulfilment of one of these fundamental safety functions.

There are many different ways of classifying accidents in NPPs. Typical classes are presented in the following.

## 2.2. CATEGORIZATION OF INITIATING EVENTS

The term 'postulated initiating event (initiating event)' refers to an unintended event, including operating errors or equipment failures, which, directly or indirectly, endangers fundamental safety functions. Typically, such an event necessitates protective actions (automatic, manual, on-site and/or off-site) to prevent or to mitigate the undesired consequences to plant equipment, plant personnel or the public.

Because of the many possibilities for the loss and/or degradation of fundamental safety functions, the development of a comprehensive list of initiating events is a complex task needing the use of operational experience, engineering judgement, PSA studies and deterministic analysis of accidents.

Nevertheless, setting a list of initiating events, even temporarily, is important to ensure a sufficient scope of analysis of a plant response to postulated disturbances in process variables, to postulated malfunctions or failures of equipment and to human failures. Accident analysis is intended to help determine the course and consequences of the event and to evaluate the capability of the plant and its personnel to control or to accommodate such conditions.

For the purposes of accident analysis, it is reasonable to group all initiating events into categories. There are different sets of criteria for grouping, thus leading to different event lists. The most typical categories used in DBA are based on grouping by:

(a) Principal effect on potential degradation of fundamental safety functions,
(b) Principal cause of the initiating event,
(c) Frequency and potential consequences of the event,
(d) Relation of the event to the original NPP design (for existing plants).

Grouping by principal effect leading to potential degradation of fundamental safety functions leads to the following event categories [11], considered typically in the reactor design:

- Increase in heat removal by the secondary side,
- Decrease in heat removal by the secondary side,
- Decrease in flow rate in the reactor coolant system,
- Increase in flow rate in the reactor coolant system,
- Anomalies in distributions of reactivity and power,
- Increase in reactor coolant inventory,
- Decrease in reactor coolant inventory,
- Radioactive release from a subsystem or component.

Each category of events is typically subdivided into several more specific events. Events which are expected to occur during the plant lifetime are called anticipated operational occurrences (anticipated transients). They are also analysed under the assumption of a complete failure of the fast reactor shutdown system (an anticipated transient without scram (ATWS)). Additional variations for each individual event are obtained by considering various plant operational states at the time of the accident. 'Radioactive releases' include events which do not represent the consequences of another event given above; i.e. the release is a direct result of the failure of the component which contains radioactive material.

Grouping by principal cause of the initiating events considered in the reactor design leads to the following categories (see, e.g., Ref. [5]):

- Reactivity anomalies due to control rod malfunctions,
- Reactivity anomalies due to boron dilution or cold water injection,
- Coastdown of the main circulation pumps,
- Loss of primary system integrity (LOCAs),
- Interfacing systems LOCA,
- Loss of integrity of secondary system,
- Loss of power supply,
- Malfunctions in the primary systems,
- Malfunctions in the secondary systems,
- ATWSs,
- Accidents in fuel handling,
- Accidents in auxiliary systems,
- Accidents due to external events.

A subdivision of the individual groups above into up to 15 events is sometimes used.

Grouping by relation of the event to the original plant design leads to the following categories [5]:

(a) Anticipated transients and postulated accidents considered in the original design, which may need to be reanalysed according to new methods.
(b) Anticipated transients and postulated accidents not included in the original design, which may need to be analysed for a safety upgrading of the plant (called 'safety upgrading accidents'); these events also need to be analysed with the same new methods, to the extent practicable.
(c) Postulated accidents not included in the original design because of their assumed low probability of occurrence; these can be analysed using best estimate methods that account for the actual frequency of the event, its consequences and associated uncertainties.

Grouping by frequency of the occurrence of an event differs in different countries. One of the possible subdivisions is given in Table I. The probabilistic values given in the table are illustrative: they are to be considered more qualitatively than quantitatively. Usually, there is a close interrelation between probability of occurrence and acceptance criteria. One method of quantifying the frequency of event consequences is by means of a Level 1 PSA. Probabilistic safety analysis identifies not only the sequences leading to core degradation, but also the more frequent sequences which lead to no, or to limited, plant damage. Although a PSA is often used to identify severe accident sequences, it is not necessary to do a PSA before doing a severe accident analysis. 'Generic' severe accident sequences, in which the core damage state is defined from the outset, may be used to test the capability of the containment and to design mitigatory features such as debris spreading and/or flooding areas.

Beyond design basis accidents and severe accidents (not covered by the previous discussion) are typically treated separately in accident analysis, although some initiating events are the same. The results help to determine measures to prevent severe accidents and to mitigate the radiological consequences. Accident management and emergency response measures are necessary if all the barriers against radioactive releases are significantly degraded in a BDBA. For severe accidents, containment and/or confinement typically remains as the only barrier to limit accidental releases. The measures to restore and maintain the safety functions under such conditions include the use of:

(1) Alternative or diverse systems, procedures and methods (e.g. in-vessel melt retention), including the use of non-safety-grade equipment;
(2) External equipment for temporary replacement of a standard component;
(3) Off-site emergency measures (limitations on food consumption, taking shelter and evacuation).

TABLE I. POSSIBLE SUBDIVISION OF EVENT OCCURRENCES

| Occurrence (1/reactor year) | Characteristics | Terminology | | Acceptance criteria |
|---|---|---|---|---|
| $10^{-2}$–1 (Expected in the life of the plant) | Expected | Anticipated operational occurrences | Anticipated transients, transients, frequent faults, incidents of moderate frequency, upset conditions, abnormal conditions | No additional fuel damage |
| $10^{-4}$–$10^{-2}$ (Chance greater than 1% over the life of the plant) | Possible | DBAs | Infrequent incidents, infrequent faults, limiting faults, emergency conditions | No radiological impact at all or no radiological impact outside the exclusion area |
| $10^{-6}$–$10^{-4}$ (Chance less than 1% over the life of the plant) | Unlikely | BDBAs | Faulted conditions | Radiological consequences outside exclusion area within limits |
| $<10^{-6}$ (Very unlikely to occur) | Remote | Severe accidents | Faulted conditions | Emergency response needed |

A very high number of individual accident scenarios can be derived from combinations of event categories, plant operational states, applicable acceptance criteria, etc. Complete computational analysis of all the resultant scenarios is not practicable. It is therefore suggested to select from each event category a reasonable number of limiting cases which present the greatest challenge to the relevant acceptance criteria and which define the performance parameters for safety related equipment. These limiting (bounding and enveloping) cases need to be analysed in detail and reported to the regulatory body. The selection of limiting cases can be based on more detailed calculations, on qualitative comparison with other events or on engineering judgement.

The concept of bounding cases is often used in licensing analysis. For other purposes, such as development of the documentation for plant operations or for probabilistic studies, more realistic analyses are used.

Note that none of the aforementioned methods guarantees the identification of a complete set of accidents. Generally a combination of methods is used, supplemented by a review of:

- Accident analyses done for similar designs;
- Engineering judgement and expert reviews;
- 'Bottom up' methods such as failure modes and effects analyses;
- Real operating experience to determine the reliability of equipment;
- 'Near misses' or precursor events;
- Actual events.

## 3. ACCEPTANCE CRITERIA

Acceptance criteria are used to judge the acceptability of the results of safety analysis. They may:

- Set numerical limits on the values of predicted parameters;
- Set conditions for plant states during and after an accident;
- Set performance requirements on systems;
- Set requirements on the need for, and the ability to credit, actions by the operator.

Acceptance criteria are most commonly applied to licensing calculations, both conservative and best estimate. Acceptance criteria may also be applied to the results of severe accident analyses, typically in terms of doses to the public or the prevention of consequential damage to the containment. The range and conditions of applicability of each specific criterion have to be clearly specified.

*Basic (high level) acceptance criteria* are usually defined as limits by a regulatory body. They are aimed at achieving an adequate level of defence in depth. Examples would be doses to the public or the prevention of consequential pressure boundary failure in an accident.

*Specific acceptance criteria*, which may include additional margins, are often developed as well. These acceptance criteria are chosen to be sufficient but not necessarily to meet the basic acceptance criteria. Typically they are used to confirm that there are adequate safety margins beyond the authorized limits to allow for uncertainties and to provide defence in depth. They may be developed by the designer and/or owner and approved by the regulatory body; or they may be set by the regulatory body itself. An example of the latter would be a limit on the cladding temperature in a LOCA in a PWR.

The analyst may set *analysis targets* at an even more detailed level (more demanding acceptance criteria) to simplify the analysis (e.g. to avoid having to do

very sophisticated calculations) or to limit economic loss from anticipated occupational occurrences. An example would be the prevention of fuel dryout under 'best estimate' assumptions for a loss of flow.

In some jurisdictions the regulatory body may approve the whole set of acceptance criteria (basic acceptance criteria, specific acceptance criteria and sometimes even analysis targets). In other jurisdictions the regulatory body may not formally approve the more specific criteria or analysis targets but review the choices made by the applicant.

Acceptance criteria vary according to the conditions associated with the accident, for example, the frequency of the initiating event, the reactor design and the plant conditions. Different criteria are generally needed to judge the vulnerability of individual barriers and for various aspects of the accident. More stringent criteria apply for events with a higher probability of occurrence, as indicated in Table I. For example, a 'no consequential containment damage' criterion is appropriate for all DBAs, whereas a 'no cladding damage' criterion would only be appropriate for frequent accidents and anticipated operational occurrences. Similarly, a 'no boiling crisis' criterion is appropriate for anticipated operational occurrences whereas a 'cladding temperature less than 1204°C' criterion is used for LOCAs.

The appropriate margin between a result predicted from accident analysis and the acceptance criteria is related to the uncertainties in the accident analysis. If a result has low uncertainty, the margin with the acceptance criteria can be smaller (e.g. the departure from the nucleate boiling ratio criterion), and conversely. A demonstration that the margin for the acceptance criterion is appropriate or sufficient can be achieved by qualitative or quantitative means:

(1) Using a conservative accident analysis to meet the acceptance criteria: This approach is 'conservative' but by an unknown amount, and gives distorted information on how the plant would respond in reality.
(2) Using more realistic accident analysis but choosing detailed analysis targets which are below the acceptance criteria: The plant behaviour is more realistically represented but the actual margin between the analysis target chosen and the specific acceptance criterion may be hard to quantify. For example, a 'realistic' model of containment thermohydraulics may be used, but the analysis target could be set at a pressure not exceeding a value somewhat below the design pressure.
(3) Using best estimate accident analysis plus uncertainties to meet the acceptance criteria: The advantage of this approach is that predicted safety margins can be expressed in quantitative terms (e.g. confidence levels). This may need more effort and computation time. In Annex II this subject is discussed in more detail and suggestions are provided which can help to reduce the effort necessary.

The acceptance criterion may or may not be set independently of the specific method of analysis, depending on the national regulatory practices. In some cases the method is prescribed, and the analytical assumptions may also be prescribed for each acceptance criterion. In other cases the regulatory body may prescribe only the acceptance criteria and the onus is on the applicant to justify the analytical method and the assumptions.

Examples of basic acceptance criteria for DBAs are as follows:

(a) The dose to individuals and the public must be less than the values defined for the accident class by the regulatory body. Such limits may be different for anticipated operational occurrences, postulated accidents and severe accidents. These limits are usually set together with the specifications for the duration of the calculated exposure and for the atmospheric conditions to be assumed.

(b) An event must not generate a more serious plant condition without an additional independent failure. Thus an anticipated operational occurrence must not generate an accident and an accident must not generate a more serious accident.

(c) Systems necessary to mitigate the consequences of an accident must not be made ineffective because of conditions caused by the accident. There are many specific criteria relating to this criterion, such as

  (i) The containment must not be damaged in a LOCA to the extent that it cannot perform its function because of:
    — the dynamic effects of whipping of primary coolant pipes,
    — jet forces from the break,
    — pressure generated internally by the break or by combustion of hydrogen,
    — pressure within internal compartments,
    — high temperatures due to the break or due to combustion of hydrogen.
  (ii) Emergency core cooling (ECC) pipes must not be damaged by the dynamic forces in a LOCA to the extent that the system becomes ineffective;
  (iii) If the functioning of the shutdown system(s) is necessary in a LOCA, it (they) must not be damaged by the dynamic effects of the pipe break.

Some of these acceptance criteria are assessed in safety analysis; others may be the subject of specific design calculations.

(1) Systems designed for accident mitigation must not subject the plant components to loads or conditions that would exceed the design or failure limits of the components for the accident condition. These criteria must be verified by separate analyses covering the thermal and mechanical loads on plant structures and components. ECC injection could cause the water hammer effect.

(2) The pressure in the coolant systems must not cause a pressure boundary failure in addition to the accident. Additional overpressure analyses may be necessary to study the effects of failures in safety valves and relief valves.
(3) For anticipated transients the probability of failure of the fuel cladding resulting from a heat transfer crisis or for some other reason must be insignificant.
(4) For DBAs, the fuel damage must be limited for each type of accident, to ensure a coolable core geometry. Energetic dispersal of fuel must be prevented in reactivity initiated accidents.
(5) In LOCAs with fuel uncovering and heat-up, a coolable core geometry and the structural integrity of the fuel rods upon cooling must be maintained. Accordingly, limits are placed on embrittlement of the cladding by: oxidation; structural deformation of the fuel rods and other core components induced by the LOCA forces, possibly in combination with other external loads; loss of shutdown capability of the control rods; and the generation of hydrogen.
(6) If operator intervention is necessary in an event, it must be demonstrated that the operator has sufficient time, adequate emergency operating procedures (EOPs) and corresponding training, and reliable information available to initiate and complete the intended action.
(7) Sufficient time and adequate means must be available to implement accident management and emergency response following BDBAs or severe accidents.

Accident analysis needs to be continued to the point in time that the plant can be shown to have reached a safe and stable shutdown state, so that:

(a) Reactivity can be controlled normally, which means that the core is and remains subcritical.
(b) The core is in a coolable geometry and there is no further fuel failure.
(c) Heat is being removed by the appropriate heat removal systems.
(d) Releases of fission products from the containment have ceased, or an upper bound of further releases can be estimated.

Acceptance criteria vary by country in terms of their scope, range of applicability and numerical values. For example, in the USA a set of 64 generalized design criteria are prescribed [20]. Again in the USA, in Ref. [21], four categories of events together with selected acceptance criteria are defined on the basis of event frequency and potential radiological consequences. Similarly, in an IAEA report [5], acceptance criteria applicable for WWER reactors are summarized for two categories of event: anticipated operational occurrences and postulated accidents (LOCAs and ATWSs being considered as special cases). The Finnish regulatory guidelines [18], apart from other acceptance criteria, also define acceptance criteria for severe accidents. The Canadian design goals and acceptance criteria for high level safety

analysis are defined in a series of documents issued by the Atomic Energy Control Board. These consist of regulatory policy documents ('R' series) and consultative documents ('C' series); see Refs [22–24].

# 4. ANALYSIS METHODS

## 4.1. BACKGROUND

The acceptability of DBA analyses for light water reactors (LWRs) has been influenced by US regulations. The Appendix A to US Nuclear Regulatory Commission (USNRC) publication 10 CFR 50 [20] establishes the minimum requirements for the principal design criteria of LWRs. General Design Criterion No. 35 establishes that emergency core cooling systems (ECCSs) are required for cooling reactor cores in the event of a rupture of pipes of the reactor coolant system or an inadvertent opening of a relief valve or safety valve of this system.

In January 1974, the USNRC published 10 CFR 50.46 [25] establishing acceptance criteria for the ECCSs for LWRs, addressing safety limits that must be assured under LOCA conditions (see 10 CFR 50.46 (b)):

(1) Maximum zircaloy cladding temperature,
(2) Maximum oxidation of cladding,
(3) Maximum amount of hydrogen generated by chemical reaction of the zircaloy cladding with water and/or steam,
(4) Coolable core geometry,
(5) Long term cooling.

Additionally, this US law adopted a *prescriptive regulatory approach*, requiring that the evaluation models to be used in licensing accident analysis must follow the conservative requirements established on Appendix K to 10 CFR 50 [25].

After more than 15 years of comprehensive experimental effort to understand the thermohydraulic phenomena occurring during a LOCA and actuation of the ECCS, the USNRC revised 10 CFR 50.46, adopting a more *performance oriented regulatory approach*, keeping the same five above mentioned criteria (1)–(5), but offering the possibility of adopting a best estimate approach for the evaluation models.

However, additional requirements are set out for the validation of the analytical models against applicable data. Requirements are also established to identify and assess the associated uncertainties in the analytical models and input data, in such

a way that the uncertainties in the calculations can be quantified when the results are compared with the acceptance criteria, giving adequate assurance that the acceptance criteria are met.

Sometimes the literature misuses the expression 'revised Appendix K rule' since in fact Appendix K kept the same conservative approach. Regulatory Guide 1.157 [21] gives one acceptable way for the fulfilment of revised 10 CFR 50.46, providing a best estimate method as an alternative to the prescriptive and conservative approach of Appendix K.

The conservative and best estimate approaches have been used in most countries, even though regulatory bodies in different countries have tailored these approaches to fit their particular needs. Present regulations [26] permit the use of best estimate codes, but there may be added requirements for conservative input assumptions, sensitivity studies or uncertainty studies. Examples of conservative assumptions could be assumptions concerning the functional capability and/or unavailability of equipment, actions or inactions by the operator, and the initial conditions of the plant.

The approach for safety analysis of CANDU PHWRs in Canada also uses a combination of best estimate physical models and selected conservative input parameters. This ensures that the predictions of plant behaviour are not physically misleading, allowing them to be used as input to the EOPs. The use of conservative input parameters ensures that the results of the analysis are conservative with respect to acceptance criteria such as the integrity of fuel cladding or the reactivity margin for shutdown.

Although the definitions of conservative and best estimate approaches are given more precisely in national regulatory guides, the following definitions help to clarify the basic ideas used in each approach:

(a) *Conservative model:* A model that provides a pessimistic estimate for a physical process in relation to a specified acceptance criterion.
(b) *Conservative code:* A combination of all the models necessary to provide a pessimistic bound to the processes relating to specified acceptance criteria.
(c) *Best estimate model:* A model which provides a realistic estimate of a physical process to the degree consistent with the currently available data and knowledge of the phenomena concerned.
(d) *Best estimate code:* A combination of the best estimate models necessary to provide a realistic estimate of the overall response of the plant during an accident. In accordance with Ref. [26], the term 'best estimate code' means that the code is free of deliberate pessimism, and contains sufficiently detailed models and correlations to describe the relevant processes for the transients that the code is designed to model.
(e) *Conservative data:* Plant parameters, initial plant conditions and assumptions about availability of equipment and accident sequences chosen to give a

pessimistic result, when used in a safety analysis code, in relation to specified acceptance criteria.

(f) *Realistic data:* Plant parameters, initial plant conditions and assumptions about availability of equipment and accident sequences chosen to give a realistic (also 'as designed', 'as built', 'as operated') result.

(g) *Bounding data:* This category is typical of nuclear data that usually change from cycle to cycle or from the beginning to the end of a given cycle. Using such varying data, conservative results can be obtained.

In simple terms, a conservative approach is adopted to ensure that the actual plant response in relation to a selected criterion is bounded by the conservative value for that response, i.e. for the example of peak cladding temperature (PCT), the conservative approach ensures that:

$$PCT_{conservative} > PCT_{actual}$$

A best estimate approach ensures that the predicted plant behaviour with given uncertainty includes the actual value, i.e.

$$PCT_{best\ estimate} - PCT_{uncertainty} \leq PCT_{actual} \leq PCT_{best\ estimate} + PCT_{uncertainty}$$

The conservative approach may use conservative data or bounding data. In the first case, different calculations related to different states of different cycles may be needed. Choosing bounding data, i.e. covering all possible conservative data for plant states, may reduce the number of calculations needed to obtain a conservative result.

The conservative approach does not give any indication of the actual margins between the actual plant response and the conservatively estimated response. By contrast, the uncertainty estimate provided in the best estimate approach is a direct measure of such margins. As a result, the best estimate approach may allow for the elimination of unnecessary conservatism in the analysis and may allow the regulatory body and plant operating organization to establish a more consistent balance for a wide range of acceptance criteria. A conservative approach does not give any indication about actual plant behaviour, including timescale, for preparation of EOPs or for use in accident management and preparation of operation manuals for abnormal operating conditions.

Sensitivity analysis, including systematic variations in code input variables or modelling parameters, can be used, in combination with expert judgement, to help identify the important parameters necessary for an accident analysis by ranking the influence of accident phenomena or to bound the overall results of the analysis. The results of experiments can also be used to identify important parameters.

Although the acceptability of the approach to be used for an accident analysis needs to be defined by the regulatory body, the use of totally conservative approaches (conservative models, input data and plant conditions) now seems to be unwarranted given the broad acceptance of best estimate methods. Mature best estimate codes are widely available around the world, an extensive database exists for nearly all power reactor designs and best estimate plant calculations are well documented.

At the other extreme, the use of totally best estimate approaches is not always possible or desirable because of the difficulty of quantifying code uncertainties for every phenomenon and for every accident sequence. In particular, the lack of experimental data for BDBAs precludes the complete definition of code uncertainties for these accidents. A combination of approaches is therefore suggested.

The analysis of accidents with best estimate codes using combinations of best estimate and conservative inputs is particularly appropriate since this approach provides some estimates of the uncertainties in the overall plant behaviour. These estimates can then be compared with the uncertainty estimates developed through relevant activities in different countries in code validation, as well as studies on representation and uncertainties in plant data, to help to establish confidence in the predicted behaviour of the plant. This approach is dependent on the continued emphasis on activities in development and validation of best estimate codes to ensure that such codes can be used with a high degree of confidence.

Since the activities in the development and validation of best estimate codes have focused primarily on LWR designs, it is important that those organizations analysing alternative reactor designs using best estimate models developed for LWR designs take into account any design specific features or conditions that may alter the applicability of those models and their associated uncertainty estimates.

## 4.2. CONSERVATIVE ANALYSES

Although the trend in accident analysis has continued to move to best estimate analysis rather than conservative analysis, conservative approaches [20] are still used. For example, fuel behaviour codes and vendor licensing code versions [27–29] still include options to select conservative models. Conservative modelling approaches are also used to a large extent in analysis of BDBAs simply to avoid the cost of developing a more realistic model, even though specific conservative models are not specified by regulation. In practice, conservative models are selected and evaluated on a case by case basis.

For the rigorous application of conservative approaches to DBAs, a formal procedure is normally specified. For example, the US regulations [20] define very specifically the approach to be taken, including the specific type of physical model

and the correlations to be used to ensure an adequate level of conservatism. Under this approach, the following general categories are considered [5]:

**Initial conditions.** These are parameters which can be measured directly in the plant, or calculated, which define the state of the system before the accident. Examples include power, power distribution, pressure, temperature, flow and fuel burnup. For conservative analyses, those initial conditions are selected which give conservative results for the parameters for which the acceptance criteria were selected. The selection may be based upon specified confidence limits for the uncertainties for those parameters. The specific parameters that are necessary depend upon the methods used to analyse the transients or accidents.

Not all parameters can be selected in a way that is always conservative: for example, minimizing the removal of containment heat is conservative for predicting peak pressure but non-conservative for predicting a safety signal relating to high containment pressure. Independent selection of all the various parameters in a conservative way can lead to inconsistent data, which may not be appropriate for computational analysis. If this is the case, it is suggested to select conservatively those parameters which have the strongest influence on the results for the acceptance criterion under consideration. The remaining parameters can be specified consistently afterwards. In this situation, several calculations are recommended, each accounting for one desired conservative result, so that all the bounds can be mapped.

**Availability and functioning of systems and components.** The availability of systems and components for operational transients and DBAs is generally based upon the single failure criterion (in some cases, double failure — 'failure + repair' — is also considered, for example, in Germany and Switzerland). This criterion stipulates that the safety systems be able to perform their specified functions even if a single failure occurs within the systems. An example would be the failure of one emergency diesel generator needed to run the ECCS pumps in the event of a LOCA. The single failure criterion is normally applied to active systems rather than to passive systems. For BDBAs, the single failure criterion is not appropriate, and the reliability and failure modes, including common cause failure (CCF) of the equipment, need to be determined by probabilistic methods.

The analysis also needs to include those failures that could occur as a consequence of the event itself. If such failures can occur, they must be considered in addition to the single failure. In general, equipment not qualified for specific accident conditions would be assumed to fail unless its normal operation leads to more conservative results.

In addition to a single failure and any consequential failures, postulated accidents are often analysed for a loss of off-site power. This may be assumed to occur conservatively either at the initiation of the event or as a consequence of reactor and turbine trip. A more realistic analysis would consider the electric grid reliability, and the reliability of the plant in switching from the station to the grid

transformer, to determine compliance with the acceptance criteria for an accident with loss of off-site power.

In most cases, control systems serve to mitigate the consequences of an event. Thus, it is often conservative to assume that the automatic features of the control system do not function. However, in certain situations, the control systems may aggravate the transient or delay actuation of the protection features. The analyst needs to investigate these situations (not necessarily performing detailed calculations), starting with the assumption of full operability of control systems.

The analyses also need to take into account conservative values for the delay in actuation of the safety systems, for protection set points and for key parameters of the safety system (such as the flow rates of the ECCS and the safety valves). The choice would be related to the conditions under which action would be taken at the operating station to shut down the plant and/or the level of intervention of the safety system would be determined.

**Operator actions.** For conservative analyses it is normally assumed that operator action does not take place for a prescribed period of time, but that after this the action takes place successfully. Operator failures, apart from those specified as initiating events, are not normally considered in anticipated transients or DBAs but may be considered part of BDBAs or in PSA. In some countries (such as the Russian Federation) operator errors are directly taken into account.

Considering the operator action to be correct could be justified by fulfilment of all the following conditions:

(a) Sufficient information is provided to the operator by the available instrumentation or by other symptoms that allow unambiguous diagnosis of an event.
(b) The necessary action is clearly described by the corresponding operating procedure.
(c) The equipment needed by the operator for restoration of the plant to a safe state is available.
(d) The operator has adequate training to perform the action.
(e) The operator has a sufficient time margin (usually at least 15–30 min) to diagnose the event and to take proper corrective action.

**Computer codes and models.** Specific conservative models and correlations are used that have been demonstrated to provide pessimistic estimates of the response of a plant. For example, correlations for oxidation of fuel rod cladding are specified that provide an upper bound on the amount of heating and on the extent of cladding oxidation in a specified accident. Conservative models are normally used in combination so that it is assumed that the conservative conditions occur simultaneously for all the phenomena represented by the conservative models.

For example, it might be specified that conservative estimates for heat generation due to both cladding oxidation and decay heat be used, so that the resulting rates of fuel rod heating are increased by both conservative estimates.

## 4.3. BEST ESTIMATE ANALYSES

Best estimate analyses provide a good view of the existing margins or limits on NPP operation in relation to safety analyses. The use of a best estimate code is essential for a best estimate analysis. Such codes do not include models that are intentionally designed to be conservative. The system thermohydraulic codes and beyond design basis codes are widely used by regulatory and research organizations [30–34]. In some cases, the user can 'tune' the models in the code to force the code to provide conservative results. However, this is usually only necessary in special circumstances in which the uncertainties are not known or are unacceptably large. Fuel behaviour codes are also considered to be best estimate codes even though some of these codes still contain options to select conservative models. The codes may have very different qualification levels for reasons such as the different experimental data available for qualification and the different extents of independent assessment.

The best estimate approach is highly dependent upon an extensive experimental database to establish confidence in the best estimate codes and to define the uncertainties that have to be determined for the best estimate results. For DBAs this database is sufficiently extensive, mainly for LWR conditions, and it is growing for advanced LWR and other reactor designs. For BDBAs, the database is more limited but is still extensive, particularly for the early phase of accidents during the initial heating and melting of the core and the latter phases of accidents in which the response of the containment is critical. Code to data comparisons are an important part of the best estimate approach, in particular in determining code bias and uncertainties.

The best estimate approach for the determination of code biases and uncertainties also utilizes comparisons of best estimate code calculations with the data from operating plants. However, the applicability of these comparisons for the purpose stated here needs to be given adequate consideration, owing to the limitations of the plant instrumentation, in the light of knowledge of the plant status and in data recording in relation to accident conditions.

Estimations of code uncertainties are performed in a variety of ways. A detailed best estimate approach for thermohydraulic analysis of design basis systems is outlined in the USNRC Regulatory Guide already referred to [20]. Detailed methods for determining the uncertainty estimates for best estimate calculations and application of the methods to small and large break LOCAs are presented in Refs [35, 36]. Different approaches are also discussed in the following sections and, in particular, in Annex II.

## 4.4. SENSITIVITY AND UNCERTAINTY

Although the definitions of sensitivity, uncertainty and probabilistic analyses vary, in this Safety Report they are meant in the following way:

(a) Sensitivity analyses include systematic variations in code input variables or modelling parameters to determine the influence of important phenomena or models on the overall results of the analysis, particularly the key parameters for an individual event.
(b) Uncertainty analyses include the estimation of uncertainties in individual modelling or in the overall code, uncertainties in representation and uncertainties in plant data for the analysis of an individual event. Scaling studies to quantify the influence of scaling variations between experiments and the actual plant environment are included in this definition. In some references, code scaling and uncertainty analysis are identified separately. The evaluation of uncertainty, restricted to design basis analyses, is discussed in Annex II.
(c) Probabilistic analyses are performed to quantify the consequences of the end points of PSA sequences. Because there can be many such sequences, they are usually grouped into categories, and one representative or bounding analysis is performed for each category.

The results of sensitivity analyses using arbitrary variations in input or modelling parameters are sometimes inadvertently misinterpreted as code uncertainties. However, such an interpretation is really only valid if the variations reflect the uncertainty estimates in significant parameters and if the uncertainties in the models used to propagate the results of such variations are negligible.

Expert judgement and early sensitivity studies have identified which accident sequences need to be included in analyses of DBAs and, in some formalized approaches, which phenomena need to be considered in the estimation of code uncertainties. In some cases, sensitivity options have been included in the codes which allow code users to obtain results of best estimate analyses together with sensitivity estimates associated with important code input parameters. Because of the computational effort necessary, such options have not typically been included in system thermohydraulic codes. Sensitivity studies have been used in combination with best estimate analyses to provide bounding results where the uncertainties in important models were unknown but could be bounded.

For the systems thermohydraulic codes used for analysis of DBAs, several different formal methodologies have been developed to help evaluate the uncertainties in their predictive results. These methodologies have been characterized in Ref. [37] as falling within three basic approaches for quantifying the uncertainties in the code calculations. The first approach uses a combination of expert judgement,

statistical techniques and multiple calculations of code sensitivity to combine uncertainties in key parameters, initial and boundary accident conditions, and scaling effects. The second approach uses scaled experimental data and code with data comparisons to estimate uncertainties in predicted plant behaviour. The third approach uses bounding calculations. The general implementation of such approaches is further discussed in Section 6.5, which describes representative code validation programmes, and in Annex II, which gives more details on uncertainties in representation and in plant data.

One of the most comprehensive methodologies used for system thermohydraulic codes is the code scaling, applicability and uncertainty (CSAU) approach as outlined in a USNRC Regulatory Guide [38]. Because of the need for an extensive database, scaling studies, expert assistance to estimate the relative importance of accident phenomena and a large number of code calculations, this approach has been applied only to a limited number of accidents, including small and large break LOCAs [35, 36].

Different methodologies have also been developed for the estimation of code uncertainties for best estimate fuel behaviour codes under DBA conditions. Because a large number of experiments have been performed using prototypic fuel rods under a wide range of conditions, direct estimation of code uncertainties is possible through extensive code to data comparisons. Different techniques have been used to describe uncertainty results, including scatter plots and statistical uncertainty estimates of both the bias and random components of uncertainties. In some cases, the results are presented in terms of different combinations of best estimate models, so that code users can select the best combinations depending on the accident conditions being considered.

The development of best estimate fuel behaviour codes in developed countries has been limited since the early 1980s. There are virtually no active programmes on the estimation of the uncertainties in best estimate fuel behaviour codes, although programmes may be started in future (e.g. the CAPRI project in the international framework of the Organisation for Economic Co-operation and Development) to address recent concerns about the behaviour of upgraded nuclear fuel, including its operation under extended burnup conditions. Such programmes are ongoing or under preparation in the Russian Federation [39].

Different uncertainties from different sources affect any such calculations. Uncertainties arising from plant operation are covered in the next paragraph. Some of the overall uncertainty sources can be eliminated through user training and careful quality assurance, for example by reducing the ‘user’ effect and the effects of using different computer hardware or operating systems. Others, such as the degree of acceptable spatial and temporal convergence (the capability of a code nodalization to produce converged results when the spatial mesh dimensions and the time steps are reduced), must be determined and possibly eliminated prior to accident analysis

through analytical convergence studies. Some uncertainties related to model structures are difficult to quantify formally and may be impossible to eliminate. The use of steady state developed and qualified correlations for transient calculations may also introduce uncertainties which cannot be estimated. The analyst needs to attempt to reduce the effects of such uncertainties upon the predictions (see also Section 7) but must be aware that they cannot be totally eliminated.

Uncertainties in plant data are important and are usually available from historical records of actual operating plants. These can be included in the statistical uncertainty analysis and may be used also for the estimation of similar uncertainties for plants that are under design. Measurements of different operational parameters with higher accuracy can also be utilized for such a purpose.

The methods developed for the estimation of uncertainties for codes for severe accident analysis are much less formal than those for design basis codes. For the early stages of accidents, for which a relatively large number of data exist for representative fuel assemblies, the direct estimation of uncertainties through code to data comparisons has been used for mechanistic codes [40, 41]. For the later stages of an accident, it is not possible to estimate code uncertainties from code to data comparisons since the amount of data is limited. For many of the phenomena important for these stages of an accident, the results from the Three Mile Island (TMI-2) accident in the USA in 1979 are the main data available to assess the applicability of models. Unfortunately, because important thermohydraulic boundary conditions for the TMI-2 accident are known only to a limited degree, it is only possible to establish qualitative estimates of the code uncertainties for these phenomena.

In a limited number of cases, including heat transfer within molten pools and debris beds and on the exterior of vessels, a combination of small scale thermohydraulic experiments and experiments with simulant materials could be used to estimate the uncertainties in important processes. However, such estimates have not been performed on a systematic basis. Comparisons between the systems codes and the more detailed phenomenological models, engineering judgement and code to code comparisons have been used to estimate the uncertainties in individual models or overall code results in a limited number of cases. A scaling and hierarchy based method, as well as a pioneering approach capable of treating phenomenological uncertainties which are not quantifiable, has recently been proposed in the USA in the area of uncertainty analysis for severe accidents.

## 4.5. PROBABILISTIC ANALYSIS

The application of probabilistic techniques is not included among the main objectives of the present Safety Report. Nevertheless, a few statements are given

below in relation to the use of probabilistic techniques in the general framework of accident analysis.

It is not practical to simulate all the transient situations that may be expected in a typical NPP. Therefore, a hierarchy of transients can be achieved by using suitable probabilistic approaches. The importance of a transient is usually established on the basis of the probability of occurrence and the consequences of the accident in terms of radioactive releases. In this way, a number of transients become suitable for analysis by conservative or deterministic approaches.

Probabilistic and deterministic analyses have been combined in a variety of ways. Probabilistic analyses have also been used in individual plant examinations and risk assessments to identify the specific accident conditions to be used for best estimate analysis of BDBAs. Uncertainties in modelling, sensitivity studies and probabilistic analyses were combined to determine the likelihood of containment failures associated with direct containment heating.

Examinations of individual plants and probabilistic risk assessments are not always necessary to obtain estimates for code uncertainties for a range of conditions, owing to similarities in plant designs and accident initiators and the relatively extensive data from assessments that are currently available from around the world. However, best estimate analyses and uncertainty analyses are important components of a comprehensive risk assessment or plant examination.

The main focus of PSA is to provide realistic answers, so best estimate codes and data are normally used. However, the results of the supporting analysis may sometimes be 'bounded' by the results of deterministic or conservative analyses to show that equipment performance is satisfactory; such analysis is not to be used for designing EOPs.

# 5. TYPES OF ACCIDENT ANALYSIS

The results of safety analysis are used in a number of different areas. For each use, this section sets the objective, explains the application, describes the relevant part of the project stage in which the results are used, summarizes typical assumptions and suggests the scope of the analysis.

## 5.1. DESIGN ANALYSIS

Design analysis is used in the design of a new plant or in modifications to the design of an existing plant, so that the designer can confirm that the design meets the relevant national safety requirements.

Design analysis is done to assist in setting characteristics such as:

(a) Equipment sizing, including determination of parameters for pressure, temperature, electric power, flow and cooling for safety related equipment, such as the ECCS, containment sprays and emergency water supplies;
(b) Approximate determination of set point values for parameters which trigger protective systems, to confirm that they are effective and allow adequate operating margins;
(c) Assessment of dose to the public, for confirming such aspects as containment leak rate and radius of the exclusion area boundary of the plant.

Design analysis is also used to check at an early stage that the design will meet national licensing requirements. The safety analyst works closely with the designer so that the design configuration can be optimized in terms of safety and cost. The process is iterative.

Design analysis is most effective when performed at the conceptual design stage, as soon as basic plant parameters have been proposed. Safety analysis at this stage can provide guidance to designers and avoid time wasted in developing details of a design which may later have to be changed. It is generally far more expensive to change a design than to repeat a safety analysis once detailed design has begun.

Normally a conservative approach is used for design analysis, including making conservative assumptions on plant data, system performance and system availability. The same computer code package that is used for licensing analysis is also used at the design stage. Ideally the codes would be validated for the application. However, not all the plant's physical data will be well characterized, and some may be missing altogether; in this case the safety analyst and the designer would need jointly to agree on and record reasonable assumptions for the missing data.

A quality assurance system needs to be in place so that when the data are finally developed they are cross-checked against these assumptions, and, if necessary, the safety analysis is redone. Other data (such as balance of plant data) may not be available at all much before project commitment. In this case the *assumptions* used in the safety analysis are based on past practice and the project technical description, and become *requirements* on the balance of plant, to be specified in the contract. In addition, the plant models, such as those of plant control and novel components, may be only partially developed, and again 'reasonable' assumptions need to be made. If the plant has novel components or operates under different conditions, the code package may not be sufficiently validated; models may then be developed and used in the application, before adequate validation is complete (this poses a threat to the schedule which must be assessed in the project).

The same acceptance criteria as are used for licensing analysis are used in design analysis to ensure that the product can be licensed. Other acceptance criteria

may be specified by the customer. However, the safety margins demonstrated at an early stage in the design may erode as the detailed design progresses, owing to such factors as:

(1) Design modifications (e.g., arising from the need to minimize plant costs or constraints due to the allocation of physical space or electrical loads);
(2) Results from research and development;
(3) Results from plant operating experience;
(4) Results from safety analysis owing to the refinement of predictive models.

It is therefore prudent, and careful consideration needs to be given on a case by case basis, to include extra margins in the safety analysis (compared with the acceptance criteria) beyond those prescribed for safety and licensing, as a contingency. These margins can be reduced as the detailed design nears completion, also in consideration of past experience.

The scope of an analysis is set by the equipment characteristics that have to be determined and also by the need to ensure that the product can be licensed. It is not necessary or cost effective to do a preliminary analysis of all DBAs. Instead, past experience and judgement are used to select those accidents for which the margins have been historically small and which set major performance requirements for the reactors and equipment. For example, large LOCAs would be analysed early in the design of any new plant, whereas loss of feedwater might not. Even within a class of accidents, such as large LOCAs, not all cases would be analysed; only those with the smallest margins or the bounding cases. Even for bounding cases, not every phase of the accident need be analysed; for example, a steam line break inside the containment would certainly be analysed to the point of predicting peak pressure and temperature in the containment, but the calculation of potential doses to the public could be deferred until the analysis for licensing.

Design analyses to support modifications to an existing plant can be more limited in scope, since it is usually clear from the safety analysis report (if it is available with adequate format and content) which accident sequences are affected. The plant PSA (if a PSA has been performed) can be used in determining *all* accidents which credit the equipment being changed, from which the most important accidents can be selected. In such a case, the assumptions discussed earlier apply in general, although the rest of the plant will be well characterized.

IAEA Safety Requirements [1] (see also the related Safety Guide [3]) require that accident analysis for NPP design as part of the safety assessment, under the responsibility of the operating organization, be independently verified by a team of experts who are, as far as practicable, independent of the designers. This verification is in addition to the QA process carried out in the design organization.

## 5.2. LICENSING ANALYSIS

Licensing analysis is used in the design of a new plant, or in modification of the design of an existing plant, to provide evidence to the regulatory body that the design is safe. Regulatory bodies may require new calculations when new evidence arises from experiments or from operational experience at the plant. Regulatory bodies may also require the use of updated computer codes which incorporate results arising from new experiments or from operational experience at the plant.

The acceptance criteria used in licensing analysis are defined either by the regulatory body or by the designer and accepted by the regulatory body. In the latter case, it is the practice in some countries to reach agreement with the regulatory body on the acceptance criteria before the analysis is started.

For a new plant, preliminary licensing analysis is performed prior to and as a condition of awarding the construction licence; and final licensing analysis is performed prior to and as a condition of awarding the operating license. For modifications to an existing plant, the final licensing analysis is performed prior to connection and/or use of the equipment; for major changes, it may be a requirement to submit a preliminary licensing analysis before construction of the modification. Licensing analysis for an existing plant may also be a requirement if its current safety assessment needs revision owing to results from research and development, from plant operating experience (e.g. results on the effects of ageing) or from the refinement of predictive models.

Historically, a conservative approach has been taken for licensing analysis, including making conservative assumptions on plant data, system performance and system availability. The assumptions and acceptance criteria used in current licensing analysis are prescribed nationally and are covered in other sections of this Safety Report.

At the stage of issuing the construction licence, the plant data have to be relatively well defined. Some details (e.g. of the design of the control system) may be missing; this can be addressed by using ‘reasonable’ values, which have to be confirmed, or the results shown to be insensitive to the value chosen, at the operating licence stage. Computer codes have to be validated in their area of application. Research and development may still be continuing to confirm the behaviour of new components; this represents a project risk if there is no fallback alternative to design or safety analysis (e.g. the use of bounding analysis).

By the time an application is made for an operating licence, the plant data need to be complete and verified, and any essential validation of computer models needs to be complete. Where the safety analysis relies on operating procedures, these have to be formally recorded, or there needs to be a formal process to ensure that the assumptions from the safety analysis will be incorporated into the operating procedures.

Normally the final safety analysis is submitted in advance of commissioning. Potential changes to the assumptions in the safety analysis or data arising out of

the cold, hot and active stages of commissioning must be assessed and, if necessary, the safety analysis be revised. Usually such changes can be introduced without reanalysis, but a formal review and/or disposition process is needed.

For modifications to, or reassessment of, an existing plant, the methods and assumptions used in the original licensing submission may need to be changed, for several possible reasons:

(a) The original licensing basis may not be the same as that used in newer plants. The acceptance criteria may be determined from a regulatory backfit or cost–benefit policy, if one exists, or by negotiation with the regulatory agency on a case by case basis before a committment has been made to make the modification.
(b) The safety analysis tools used on the original plant may have been superseded by more sophisticated tools.
(c) The original plant licensing basis may have been recognized as inadequate or may no longer be met.

Detailed guidance covering each of the topics discussed here is outside the scope of this Safety Report, as decisions will be determined by national policy and national circumstances. However, the following approach has been used in some countries for safety analyses of existing plants:

(1) Use of up to date safety analysis tools, since they best represent real physical behaviour.
(2) Use of 'as built' plant data (confirmed in the field if necessary) and 'as operated' system parameters and limits.
(3) Use of the plant PSA to determine risk dominant sequences (relevant to the modification in question, if the analysis is due to a modification).
(4) Development of at least a screening cost–benefit assessment in which the benefit is based upon the results of different safety analyses.
(5) Use of best estimate codes and data where practical so that any cost–benefit assessment of the backfit is not biased by overconservatism in the analysis.
(6) If best estimate codes are used, a sensitivity or uncertainty analysis on key parameters (those that are influenced by sensitivities or uncertainties in the plant data, the plant model and the physical models) is recommended to show that there is no large increase in risk if one of these parameters is changed within its uncertainty band. The uncertainty allowance for plant parameters needs to be derived from operating experience rather than from the values used in the original licensing analysis.

As with safety analysis assumptions, the scope of licensing analysis is determined by national requirements and practice. For new plants, a comprehensive identification

and analysis of all DBAs is necessary; however, if one sequence can be shown to bound other sequences, less effort is needed on the latter. The results are compared with regulatory acceptance criteria. For modifications to existing plants, a licensing analysis more limited in scope may be undertaken (a subset of the licensing analysis), restricted first to those sequences directly affected by the modification, and possibly to the risk dominant subset thereof. In this case, a systematic review of accidents, also making use of the existing final safety analysis report or the PSA of the unmodified plant, may establish confidence that the subset has been appropriately selected.

## 5.3. VALIDATION OF EMERGENCY OPERATING PROCEDURES AND PLANT SIMULATORS

Emergency operating procedures define the operator actions during anticipated transients and in accident conditions. Owing to the very limited possibility of using real plant transients for validation of EOPs, analyses by sophisticated computer codes are used to support the development and validation of EOPs.

The analyses used for EOP development are basically either preparatory or validation analyses:

*Preparatory analyses* are needed to confirm the selection of recovery strategies, to provide the necessary input for operator actions and to resolve other open issues in the review of accident mitigation strategies. The scope of such analyses is to provide the plant specific calculations needed for the development of EOPs. The analyses need to be performed in sufficient detail to define the changes in strategy or to resolve the additional specific items. During the development of the strategy, sensitivity analyses on the timing of operator actions need to be performed. The results of the analyses are used for the assessment of time margins and the optimization of procedures.

After the development of EOPs has been completed, a *validation analysis* needs to be performed. These analyses confirm that the actions specified in the procedures could be followed in the appropriate time and manner by a trained operator and that the expected response of the system is achievable, resulting in the final safe state of the reactor system. Possible failures of the plant systems and of the operator need to be considered for such analyses.

Both preparatory and validation analyses can be performed using a best estimate approach, including:

- Best estimate codes and models,
- Best estimate data,
- Best estimate assumptions.

Considerations of the most probable response of both plant systems and operators need to form the base case of the analysis. Reasonable agreement of calculations with reality is most important, while the speed with which calculations are made is less important.

Analysis performed for development and/or validation of EOPs needs to have the following additional specific characteristics:

(a) The accident sequences selected for development and/or validation of EOPs can be used in PSA analysis, including loss of off-site power, which could significantly change the course of an accident.
(b) If the strategy applied allows the operator to choose among various systems which have similar safety functions, an analysis considering various possibilities and combinations of such systems needs to be performed.
(c) If the values of certain parameters can affect the necessary actions significantly, sensitivity studies need to be performed.
(d) The available plant instrumentation needs to be modelled in order to confirm that the event can be diagnosed and to check the steps in the procedure.
(e) In the calculations, the performance of systems (e.g. instrumentation) not included in the model used, but potentially affecting the course of the accident, needs to be considered; in some cases, for instance, this can be accounted for by changing the input sequence of events in the code model considered or by assuming a range of variation for any relevant parameters.

An alternative approach is pursued in some countries (e.g. France), where the development of EOPs is based upon on a ‘state oriented approach’, which allows diagnosis using predefined state criteria. In this case, sequences based on PSA are used for checking EOPs.

Analysis to support the validation of plant simulators is used to verify the accuracy of the simulator primarily for operational transients and DBA conditions. In this case the use of plant data for validation is suggested. Similarly to the case for EOPs, in order to validate the simulator performance, the real plant recorded data are not sufficient, in particular, for anticipated transients and accident conditions. Therefore, the simulator validation process could be carried out by comparing the simulator performance with the results of reference accident analyses. The purpose of accident analyses used for simulator validation is to check the timing of the processes being simulated and the accuracy of applied simulation models.

Since the algorithms used in many plant simulators are simplified relative to currently available best estimate analysis codes, the validation of the plant simulators is important in order to verify that the simulators describe the response of the plant to a reasonably accurate level. In this case, although this is not the current practice, the definition of ‘reasonably accurate’ may be established through a regulatory

requirement. The key requirement is that the information presented to the operator by the simulator not be misleading. The best estimate codes and models used for simulator validation need to have the same capabilities and scope as the simulator software and, in turn, need to have been validated against real plant data and experimental facilities.

The scope of existing full plant simulators is currently limited, in particular for BDBAs and even some classes of DBAs. These include all the situations for which there is no proof of validity for the models and the equations that are at the basis of the simulator. In this connection, best estimate analysis is important to define the conditions in which the simulator may not be used. In the event that best estimate codes are used as the basis for the plant simulators (the most likely scenario is the use of such codes on engineering workstations without simulation of plant control panels), an independent validation needs to be performed, making use of relevant experimental data and of another best estimate code. In this instance, the use of independent review and validation of the results comparable to the independent review and validation used to validate any safety analysis needs to be employed.

The scope of the validation effort may be defined through the corresponding regulations but, as a minimum, needs to cover the range of conditions for which the simulator is being used. In the event that the simulations are intended to cover accident conditions and the results of probabilistic risk assessments are available, it is suggested that the priorities for validation be established using a combination of the likelihood of events occurring and the risks associated with the events. That is, the validation needs to include, as a minimum, both the most likely events and the risk dominant events (or set of conditions).

## 5.4. ANALYSIS RELATED TO PROBABILISTIC SAFETY ANALYSIS

In the framework of PSA, groups of accidents are defined by initiating events, actuations and failures of plant systems, and human actions, including their timing. A more comprehensive explanation of the objectives and framework of PSA can be found in Ref. [42]. However, accident analysis related to PSA is an important tool for the following:

(a) To give an accurate measure of the risks associated with different scenarios,
(b) To assist in the development of EOPs,
(c) To determine whether an event sequence is successful or not.

As a minimum, the analysis has to determine the end state of an accident scenario. The end state of an accident scenario means:

(1) For Level 1 PSA, that either core integrity is maintained or there is core damage;
(2) For Level 2 PSA, that the activity source term is calculated;
(3) For Level 3 PSA, that the radiological consequences are calculated.

There are several definitions of core damage, such as major loss of fuel cladding integrity, partial core melting and overall core melting. Prevention of core damage can be considered as a success criterion for any individual accident scenario.

Similarly to PSA itself, the corresponding accident analysis can be performed at any stage of NPP construction and operation, for example, at an early design stage, at the final design stage or during plant operation. Accident analyses for various stages differ mainly in the level of knowledge of the layout and characteristics of the plant systems.

Probabilistic safety analysis typically uses a best estimate approach for evaluation of each individual scenario. It is preferable to use best estimate computer codes and best estimate analyses for the corresponding accident analyses. For consistency, the accident analysis should use the same set of assumptions as were adopted in the framework of PSA. Nevertheless, for reducing the number of scenarios to be analysed and to simplify analyses, a bounding case approach is sometimes used. The risk from the plant can be overestimated by this approach and one must be cautious in using these results as the basis for EOPs and accident management.

The spectrum of accident scenarios to be analysed for PSA is typically broader than that for licensing purposes. In a PSA, all plant operational states including shutdown modes are considered; events beyond the design basis are also taken into account and various multiple failures (beyond the single failure criterion) and common cause failures are considered. From the phenomenological point of view, the analysis is more complicated because more complex thermohydraulic and core phenomena occur. The acceptance criteria used for licensing calculations of DBAs are not applicable here. The complexity may be partially reduced when analysis is necessary to determine only whether severe core damage has occurred and not to specify the extent of core damage.

In particular, attention needs to be paid to such accident scenarios for which acceptance criteria valid for postulated accidents are exceeded. In such a case, the analysis needs to follow the suggestions in Section 5.5 as well as the corresponding subsections in Appendix I to cope adequately with issues relating to BDBAs and severe accidents. The results of PSA are also important for identifying scenarios leading to BDBAs or severe accidents.

## 5.5. SUPPORT FOR ACCIDENT MANAGEMENT AND EMERGENCY PLANNING

Analysis of accidents for supporting accident management describes the plant behaviour in conditions for BDBAs. Operator actions are normally accounted for in the assessment of BDBAs. The results from analyses of BDBAs are used to develop operator strategy, the main goals being to prevent severe core damage and to mitigate

the consequences of an accident in the event of core damage. On the basis of such analyses, guidelines for accident management could also be developed. Unit specific conditions and criteria need to be formulated to make possible the identification of the accident and the prediction of its development. Results of BDBA analyses, defining the source term and radioactive releases, could also be used for purposes of emergency planning. As already mentioned in Section 5.3, an alternative approach, i.e. the plant status approach, relies on the development of a set of specific parameters or symptoms which indicate the status of plant safety functions. The symptoms are used to guide strategies for accident management.

Analysis of BDBAs is typically performed either for operational plants or for plants at the final stage of design. For future reactors, such analysis is necessary early on because the requirements for the mitigation of severe accidents may need to be implemented as part of the reactor design.

For severe accidents, specialized codes are used to model the wide range of physical phenomena that occur, such as thermohydraulic effects, heating and melting of the core, steam explosions, molten-core–concrete interactions, hydrogen generation and combustion, and fission product behaviour. For the analyses of severe accidents, a multi-tiered approach with several interconnected codes, including detailed codes for system analysis and containment analysis, is typically used. In certain cases, detailed multidimensional system models may be necessary to describe the response of the reactor coolant system.

The best estimate approach is intended to be used to analyse the overall response of a plant under severe accident conditions, although conservative models are still used to overcome lack of information concerning molten core behaviour. The acceptance criteria for severe accidents are less prescriptive than those for DBAs. In general terms, the probability and/or consequences of severe accidents must be shown to be extremely small, although more specific criteria can also be used, for example concerning failure of the containment or the acceptability of radiological consequences.

The analyses in support of preventive accident management for severe accidents may need a greater number of plant specific data than for analyses that do not involve severe core damage. As an example, additional specific information is needed as follows:

(1) A list of systems available to operate in BDBA conditions;
(2) Activation modes of available systems (automatic or manual);
(3) Details on the location of instrumentation and control (I&C) systems and components, and their environmental qualification;
(4) A list of signals which could influence the behaviour in accidents;
(5) Set points and operating ranges of I&C systems;
(6) Detailed characteristics of the systems considered.

Understanding the capabilities and limitations of the equipment under severe accident conditions is important for proper modelling of these systems. However, unacceptable or unquantifiable uncertainty bands will affect a deterministic and/or realistic analysis of a severe accident involving serious core degradation. This constitutes an important difference in respect of thermohydraulic analysis dealing with situations before the loss of core geometric integrity, in which a realistic and qualified uncertainty analysis can be completed.

Analysis starts with the selection of accident sequences which, without operator intervention, would lead to core damage. A method for categorization of accident sequences can be used to limit the number of sequences analysed. Such categorization is typically based on several designators of the state: initiating event, shutdown status, status of the emergency core cooling, status of the secondary heat sink, status of the system for containment heat removal and status of the containment boundary.

Recovery strategies to prevent core damage (preventive measures) need to be analysed to investigate which actions are applicable to halt or to delay the onset of core damage. Examples of such actions are various manual restorations of systems, primary and secondary feed and bleed, depressurization of the primary or secondary system and restarting of the reactor coolant pumps. Conditions for the initiation of the actions need to be identified as well as exit conditions to switch over to another action.

Similarly, the strategies for managing severe accidents to mitigate the consequences of core melt (mitigatory measures) need to be analysed. Such strategies include coolant injection to the degraded core, pressurization of the primary circuit, operation of containment sprays, and use of the fan coolers, hydrogen recombiners and filtered venting available in the different families of reactors in operation. When mitigatory strategies are developed and analysed, possible adverse effects that may occur as a consequence, such as pressure spikes, hydrogen generation, return to criticality, steam explosions, thermal shock or hydrogen burn, need to be taken into account.

The method adopted in France to deal with accident management deserves a specific discussion in this context and is reported as an example. Accident management relies on the following:

(a) The team of operators with the EOPs and a set of specific ‘guides in the event of a severe accident’ in the case of degradation of the equipment: specific plant parameters and related thresholds are selected to start the relevant procedure for accident management;
(b) The safety engineer (permanently present in the plant), who uses different procedures to check independently the state of the plant and the actions of the operators;
(c) The local crisis team, which is called into operation after the occurrence of an event;

(d) The national crisis team, which is called into operation after the occurrence of an event and which receives the values of all the parameters coming from the plant. The team has computer codes available in order that it can calculate the accident evolution and rapidly simulate future states. The team can also calculate eventual source terms and radiological risks.

All the features above are aimed at supporting the team of operators to mitigate the effects of accidents and to make decisions about the necessary off-site emergency response.

In any case, in interpreting or adopting the results of accident management studies, attention needs be paid to the fact that there may be large uncertainties present.

## 5.6. ANALYSIS OF OPERATIONAL EVENTS

Accident analysis is frequently used as a tool for a full understanding of events occurring during the operation of NPPs, as part of the feedback of operational experience. According to the IAEA's Incident Reporting System, computer codes are used for analysis of about 10% of the events reported. Typical objectives of the analysis can be summarized as follows:

(a) To check the adequacy of the previous selection of initiating events,
(b) To provide additional information on the time dependence of parameters not observable directly by means of the plant instrumentation,
(c) To check whether the plant systems and operators performed as required,
(d) To check and review EOPs,
(e) To identify new issues and questions arising from analysis,
(f) To support the resolution of potential safety issues identified as a result of an event,
(g) To analyse the severity of consequences in the event of additional failures (such as severe accident precursors),
(h) To validate and adjust the models in the computer codes used for analysis.

Analyses need to be performed by means of an approach similar to that described in Section 5.3 on the validation of EOPs and plant simulators. This includes the use of a best estimate approach in the analysis. Real plant data, if available, can be used in analyses.

If there is a lack of detailed information on the plant's status, sensitivity studies with variation of certain parameters need to be performed.

### 5.7. REGULATORY AUDIT ANALYSIS

Audit analysis is generally used by regulatory bodies for various purposes:

(1) To perform an independent verification of DBAs to support the decision making process within the framework of licensing processes;
(2) To supplement, on a quantitative basis, the task of reviewing and assessing the design and operation of NPPs;
(3) To use as a tool for qualifying regulatory staff members in charge of reviewing applications of safety analysis;
(4) To check the completeness and consistency of accident analyses submitted for licensing purposes.

It is not expected that the regulatory body will always conduct a complete set of independent analyses for every submittal within the licensing process. However, the development of its in-house capacity for accident analysis gives the regulatory body greater capability in its own decision making process as well as in communication with the licensee.

As regulatory bodies are typically not legally required to perform their own quantitative assessments, they can select some spot check calculations to verify the consistency of the accident analyses submitted. Nevertheless, special care needs to be taken in comparing results obtained by the use of different codes or methods.

## 6. COMPUTER CODES

Complex computer codes are used for the analysis of the performance of NPPs. They include many types of codes, ranging from specialized reactor physics codes to mechanistic system thermohydraulic codes (see Annex IV for examples of the many types of codes). The overall adequacy of these codes has been well established since many have been widely accepted and utilized in various countries in applications related to reactor safety. However, the user of the codes always has the responsibility of ensuring that the codes are appropriate for their end use. In general terms, as described in the following paragraphs, this includes defining the appropriate levels of detail for the modelling, documentation, verification, validation and accuracy necessary for the intended use of the codes.

For the purposes of this Safety Report, the terms mechanistic code and parametric code are used to distinguish between the two general classes of codes that have been developed for the analysis of BDBAs or severe accidents. Although the descriptions and applications may vary for an individual code, the following characteristics are used.

Mechanistic codes include the best estimate phenomenological models necessary to provide an accurate prediction of the behaviour of an NPP. The modelling uncertainties will be comparable with the uncertainties in the data used to validate the code. User defined modelling parameters need to be limited in number.

Parametric codes include a combination of phenomenological and user defined parametric models necessary to describe the important trends in the behaviour of an NPP. Extensive user defined modelling parameters allow the user to bound important processes or phenomena.

Mechanistic codes have historically been used to support experimental programmes, to help resolve important technical issues associated with severe accident behaviour and to benchmark the parametric codes. The latter are intended to be relatively fast running to allow the user to perform a significant number of calculations quickly. Parametric codes also have integrated models for the reactor coolant system, the containment and the source term.

## 6.1. TYPES OF COMPUTER CODES

For anticipated transients and DBAs, these codes can be organized by the component or system being analysed and in general can be characterized into the following six categories:

(a) Reactor physics codes;
(b) Fuel behaviour codes;
(c) Thermohydraulic codes, including system codes, subchannel codes, porous media codes and computational fluid dynamics (CFD) codes;
(d) Containment analysis codes, possibly also with features for the transport of radioactive materials;
(e) Atmospheric dispersion and dose codes;
(f) Structural analysis codes.

Reactor physics codes model the core neutronic behaviour in normal conditions and accident conditions. At present, reactor physics codes normally contain two dimensional and three dimensional models of the reactor core. The use of a multi-dimensional code is necessary when local or asymmetric effects are important. These codes have historically been used in combination with system thermohydraulics codes. Recent activities have included the development of more advanced graphics–user interfaces and the merger of codes of this type with system thermohydraulics codes.

Fuel behaviour codes describe the behaviour of individual fuel rods in normal operating and in DBA conditions. Fuel behaviour codes tend to be design specific

and are typically used by regulatory and industry groups in the countries of origin. The transient codes used for accident conditions may contain modelling options for both conservative and best estimate calculations. Although recent developmental activities with applications in accident analysis have been limited, work is currently under way to extend some of these codes for the analysis of different types of fuels: high burnup and mixed oxide fuels, in particular.

System thermohydraulic codes are typically less design specific and are applied to a wider variety of designs and conditions. A limited number of these codes are widely used around the world by regulatory, research and industry organizations. The codes developed by regulatory bodies are typically used as best estimate codes and do not contain specific models for conservative analysis. However, many of the industry supported codes contain models for conservative *and* best estimate analyses. These thermohydraulic codes are characterized by mechanistic models for two fluid, non-equilibrium hydrodynamics, point and multidimensional reactor kinetics, control systems and other system components such as pumps, valves and accumulators.

These codes can typically be used to model a wide range of configurations for single pipes, experimental facilities and full plants and, in many cases, have been applied to most reactor designs around the world. Although most of these codes initially focused upon one dimensional representations of the reactor vessel and piping, two and three dimensional representations of the vessel and other coolant system structures are now being used more widely. For advanced reactor designs with passive coolant systems, the codes typically are used to describe both the reactor coolant system and the thermohydraulic behaviour of the containment. Recent developmental activities have focused on the development of more integrated graphics–user interfaces and the application of the codes to a wider variety of reactor designs. Some work has been focused on the development of simulator versions of these codes.

Subchannel, porous media and CFD thermohydraulic codes are used to analyse specific processes within reactor systems. For example, subchannel and porous media codes can be used to analyse localized flow effects in representative fuel assemblies such as the influence of spacer grids and flow blockages on local heat transfer. Computational fluid dynamics codes may be used to analyse effects such as mixing in downcomer regions. Although there may be some overlap in the capabilities of these specialized codes, subchannel and porous media codes have historically been developed and validated for specific reactor bundle designs, while CFD codes are much more general in scope. In particular, commercially developed CFD codes may not have been developed or validated specifically for reactor safety studies. Some of the subchannel codes have been combined with system thermohydraulic codes, while CFD codes have more typically been used alone. However, there have been some recent trends to merge CFD capabilities with currently available system level codes.

Containment codes may be less detailed than system thermohydraulic codes, but are also relatively independent of their design. These codes are also supported by a combination of regulatory, research and industry groups. The codes are characterized by lumped parameter thermohydraulic models, although there are some codes available with multidimensional capabilities. The codes also contain specialized models for containment systems and components, and the more advanced codes have models for hydrogen transport and combustion.

Structural analysis codes are used to describe the behaviour of the vessel, piping and containment structures under various accident conditions. For example, these codes might be used to describe the mechanical response of the reactor vessel during reflooding to determine the likelihood of vessel failure due to pressurized thermal shock. These codes are typical commercially available codes that were developed for non-nuclear applications and utilize thermohydraulic boundary conditions supplied by the reactor coolant system or containment thermohydraulic codes. Knowledge of the mechanical properties of the materials used in the nuclear industry is necessary for these codes.

As discussed in the following paragraphs, recent developmental activities have focused on the integration of the different types of codes, particularly integrating other codes with system thermohydraulic codes. For BDBAs, the codes tend to be organized by their intended application, the level of detail in the modelling, the type of system considered and, in some cases, the phenomena addressed. These codes include:

(1) Mechanistic codes for (reactor coolant) system thermohydraulics, progression of core damage and behaviour of fission products;
(2) Mechanistic codes for containment thermohydraulics, progression of damage and behaviour of fission products;
(3) Parametric codes for system response and containment response;
(4) Mechanistic separate effects codes for the analysis of separate processes such as steam explosions.

The thermohydraulic codes for mechanistic systems in BDBA conditions can also be used for DBA since, as indicated in the examples given in Annex IV, these codes are extended versions of the thermohydraulic codes for systems that are described in the following, with additional models needed for severe accidents.

The mechanistic codes developed for BDBAs can describe the behaviour of the plant during DBAs and severe accidents. In most cases, the mechanistic codes include thermohydraulic models with options developed for severe accident conditions. As a result, these codes can be used to describe a wide range of accident conditions from accident initiation to failure of the reactor vessel. Mechanistic containment codes also describe the thermohydraulics of the containment but include additional models for

severe accident conditions. Most of these mechanistic codes are supported by the regulatory bodies of the respective countries with additional support through international programmes. Recent development activities have focused on the development of improved models, particularly in the analysis of the later stages of severe accidents, the incorporation of reactor specific models for a wider variety of reactor designs, and improvements in the numerics and architecture of the codes to improve the maintainability and reliability of the codes. As for system thermohydraulic codes, enhanced graphics–user interfaces and simulator applications have received more attention in recent years.

Parametric codes typically use simplified models in comparison with mechanistic codes and are specifically intended for severe accident analysis. Some of these codes are developed and maintained by nuclear industry organizations. The remainder of the codes are developed and maintained by regulatory and research groups in the respective countries. These codes describe the response of the reactor coolant system and containment. They include integrated models for radionuclide transport and deposition so that they can be used for source term calculations. These codes make use of a range of 'user specified' modelling parameters to allow the user to simulate possible plant behaviour. Some of the codes are being developed using a two tier approach to severe accident analysis. In this approach, these codes can be benchmarked using the more mechanistic codes.

Although the selection of the codes to be used is the responsibility of the organization performing the accident analysis, internationally recognized and accepted best estimate codes are the most appropriate where possible. Although it is the responsibility of the regulatory body in each country to accept the use of such codes, the strong commitment internationally to continue to develop and validate these codes ensures that they will continue to improve and that best estimate methods using these codes will continue to be refined.

It is not possible to define the minimal set of best estimate codes that can be used under all circumstances. However, a combination of mechanistic system thermohydraulic codes, parametric codes which can be used to support probabilistic risk assessment and source term calculations, and, where necessary, fuel behaviour codes, reactor physics codes, containment analysis codes and other supporting codes as needed, seems to be reasonable. Since system thermohydraulic codes may need the most effort in terms of developing plant input models, the use of such codes, which are applicable to analysis for DBA conditions and BDBA conditions, may demand the least overall effort and cover the widest range of accident conditions.

In the event it is anticipated that a large number of calculations are needed to support comprehensive risk assessment or source term studies, the faster running parametric codes are also appropriate. The fuel behaviour codes can be used for analysis of DBA conditions and may be used to provide initial conditions for the

system thermohydraulic codes. Reactor physics codes are typically used to support the performance of the plant as well as to provide results used in the system thermohydraulic codes for accident analysis. For analysis of severe accident conditions, containment analysis codes may be necessary to estimate the time of containment failure.

## 6.2. NECESSARY CODE FEATURES

Although it is not possible to provide a detailed list of the key phenomena and code features necessary for each type of code, three criteria can be used to judge the adequacy of the codes for treating important phenomena. Firstly, the use of internationally recognized and accepted codes provides some assurance that the codes are adequate for their intended application. For example, most system thermohydraulic codes now routinely include two fluid non-equilibrium hydrodynamic models, reactor kinetics models, control system models and models of other reactor components. Secondly, particularly for codes used for analysis of DBA conditions, lists of important phenomena have been well established internationally. In many cases, documentation is available on an individual code basis that describes the relative importance of different phenomena. For codes for BDBA conditions, the lists of important phenomena (and associated code models) are less developed. However, even in this case, formal peer reviews of the individual codes as well as other internationally sponsored documents are available (e.g. the report of the French Committee on the Safety of Nuclear Installations (CSNI) [43]). Thirdly, individual codes need to be evaluated on a systematic basis, comparing the intended application of the code with the actual conditions for which the code is applied. For example, the application of parametric codes, developed strictly for severe accidents, to analysis for DBA conditions would be inappropriate.

## 6.3. DOCUMENTATION

Each computer code needs to be adequately documented to facilitate review of the models and correlations employed, and to ensure that the models for important phenomena are appropriate and are not applied outside their range of validity. The documentation would also provide a description of the uncertainties of important models and the overall code for typical applications. The code documentation would also include user guidelines and input descriptions to ensure that the user can use the software properly. Although the guidance may vary depending on the complexity of the codes and the modelling parameters available to the user, the user guidelines or validation documentation need to give the user

some guidance on the influence of important modelling parameters, recommendations for typical applications of the code, the type of nodalization to be used and the important trends to be expected.

Typically, a complete set of documentation would include:

— an abstract of the programme
— a theory manual
— a user's manual and description of the inputs
— a programmer's manual
— a validation report.

The scope of documentation may vary depending on the complexity of the code and on the applications to which it is applied. In the most comprehensive examples, multiple volumes may be necessary to describe the design and implementation of code models and correlations. In some cases, separate manuals may be provided in which the models and correlations used in individual codes are discussed. For example, the models and correlations document for each code:

(a) May provide information on its original source and its database;
(b) May describe how it is implemented in the code;
(c) May describe the expected accuracy of the models, including an assessment of any effects were the code to be used outside its basis of data, the effects of the specific manner in which the model is implemented in the code and the effects of any unique numerical features necessary to overcome computational difficulties;
(d) May provide information on the applicability of the model to the analysis of reactor systems.

In general terms the documentation for internationally recognized codes is quite extensive and in most cases includes descriptions of the key phenomenological models, user's manuals and results of assessment calculations. The system thermohydraulic codes typically have the most comprehensive documentation since these codes have extensive manuals prepared by the code developers in addition to a number of contributors of different nationalities who have provided independent reports on the results of the code assessment and validation. The documentation for the codes for accident conditions beyond the design basis is more diverse, with nearly all codes having some form of user's manual and manuals describing the theory of the model. Some of the codes also include manuals for material properties, code developer's assessment and validation, and user guidelines. Some codes also have manuals available in electronic form or through the Internet.

## 6.4. CODE VERIFICATION

Code verification, which is defined for the purposes of this Safety Report as a comparison of the source coding with its description in the documentation, has not been applied consistently to many of the codes used around the world. Since line by line verification of these large codes is a time consuming and expensive process, this process is limited to those codes which are relatively static and not subject to continual change. In particular, many industry sponsored codes have been subjected to stringent verification procedures as a consequence of the regulatory licensing process.

## 6.5. CODE VALIDATION

There is normally [26] a regulatory requirement that codes be assessed (validated) in relation to relevant experimental data for the major phenomena expected to occur. The validation relates to the confidence that can be placed on the accuracy of the values predicted by the code. The specifics of what is required will vary according to the particulars of the safety assessment under consideration.

Four sources of data are generally used to validate these codes: phenomenological data, data on separate effects (component data), integral data and plant operational data. For severe accident conditions, the availability of data is much more limited. Integral data are available for the early phases of severe accidents but data for the later phases are obtained primarily from experimental facilities for separate effects, using simulant materials in many cases. With the exceptions of data from the accidents at Three Mile Island in the USA in 1979 and Chernobyl in the USSR in 1986, no plant data are available for the validation of models for severe accidents.

For validation, certain quantities are selected for the comparison of calculations with experimental data [43]. These quantities serve as ‘indicators’ for determining whether or not a code provides satisfactory results; i.e. indicators that can be used to measure the ‘level of validation’ of a code. The identification or choice of indicators is, therefore, a crucial step in the validation. The quantification of the validation can be expressed in terms of the accuracy with which a code predicts an indicator, and it must relate to the agreement between the values of the indicators as predicted and as measured experimentally. The indicators are directly related to the physical driving phenomena of the response to the accident and are usually those code output quantities which are compared with acceptance criteria in accident analysis.

Historically, the validation of many codes has included the formulation of a model (or hypothesis), design of validation experiments, collection of experimental data, analysis of these data, comparison of experimental data with code predictions

and reformulation (if necessary) of the model. The need for the reformulation of the model and reiteration depends on whether or not the code is judged to have met the validation goals or criteria. Currently, since many experimental programmes are run independently of the activities for code development and validation, the design of experiments, collection of data and analysis of the data may be performed separately. In addition, since many of the experimental programmes have been completed, validation of new models and codes may rely very heavily on archival data sources. However, it remains important to validate the code against at least some of the experiments which have not been used directly to support the models in individual codes.

A code can sometimes predict a set of data with a high degree of accuracy and still be extremely inaccurate for other data sets. This has led to the need to develop a 'validation matrix' for each code through which different types of experimental facilities and different sets of conditions in the same facility are used for code validation.

Most internationally recognized codes have been subjected to systematic validation procedures through a number of international programmes, with system thermohydraulic codes receiving the most attention. Other types of codes have also been systematically validated, but to a lesser extent.

The system thermohydraulic codes maintained by regulatory and research organizations are still the subject of a high level of effort in this area as a result of the work of the code developers and of other international activities. Under these programmes, which include those of the IAEA, the OECD and the French CSNI, extensive experimental matrices for code validation have been established and the codes have been assessed in relation to many of the experiments that are included in those matrices. The validation exercises have also included comparisons with relevant data from plant operations and participation in international standard problems.

Many industry sponsored system thermohydraulic codes have not received the same level of attention internationally because of the proprietary nature of the codes, although their validation results are subject to licensing review by regulatory bodies. The fuel behaviour codes used for accident analysis and maintained by regulatory, research and industry groups have not received the same level of attention internationally. In many cases, this is a consequence of the relatively limited development efforts made in respect of these codes over the past 10–15 years. However, this trend may be reversed to some extent as these codes are modified to account for the influence of new types of reactor fuel.

Many reactor physics codes have also been extensively validated but, because of the proprietary and design specific nature of many of them, the level of attention internationally has been less than that for the system thermohydraulic codes and the fuel behaviour codes. Specialized codes such as the CFD codes have received little attention internationally but may have been validated on a case by case basis.

The validation of the thermohydraulic codes for mechanistic systems for severe accident conditions has been more limited than that for DBA conditions. This is due in part to the much more limited basis of experimental data for BDBA conditions as well as the greater ongoing activities in model development for these codes. Experimental validation matrices have been developed for these codes and are used by the code developers and other code users as the basis for validation activities.

In general terms, the validation of these codes thus far has been limited largely to the early phase of accidents prior to the formation of large debris beds and molten pools, since experiments of the widest diversity are available for this accident phase. In the case of the mechanistic containment codes, the validation activities have covered many of the major processes represented by the codes, although comparisons with integral data are more limited. Both the system thermohydraulic and containment codes have also been used in a wide range of international standard problem exercises.

The validation of the parametric codes is also limited by the availability of experimental data for severe accident conditions but is also the subject of co-ordinated international programmes supported by research and regulatory bodies. Validation of industry sponsored codes has been performed by the sponsoring organizations; international activities have been somewhat restricted, however, owing to the proprietary nature of these codes.

The validation processes used in the different codes are very similar, with heavy reliance placed on comparison of results predicted by the codes with data from different sources. Standard problem exercises have been important components of many of the validation activities for many of the codes. Engineering judgement and code to code comparisons have also been used. These processes have been particularly important for the codes for beyond design basis conditions in the later phase of accidents owing to the lack of relevant integral experiments.

Although many international activities have focused on the validation of system thermohydraulic codes and containment codes for the designs and conditions of LWRs, efforts have been increasing to validate these codes for other reactor designs. However, the importance of adequate code validation and the reliance on the availability of well characterized data are relevant considerations independent of the type of reactor design or the codes being validated.

## 6.6. ACCURACY OF CODES

Although the primary objective of the code validation process is to help define the accuracy of codes, such accuracy may be defined in qualitative rather than quantitative terms owing to the time and expense associated with estimation of the uncertainties in predicted plant behaviour for wide ranges of accident conditions

and designs. In most cases, expert opinion is necessary to establish the key phenomena to be included in the uncertainty analysis and to help determine the scalability of the analysis to full plant conditions. In addition, a large number of code calculations may be necessary to estimate the uncertainties in key phenomena, to make experimental comparisons and to model the behaviour of the plant.

The assessment of the accuracy of individual codes typically includes a series of steps:

(a) Identifying the important trends in the supporting experimental data and expected plant behaviour,
(b) Estimating the uncertainties in the overall code results associated with the fundamental numerical approaches used,
(c) Estimating uncertainties in key models and overall code results,
(d) Establishing sensitivities in important processes.

As described in Section 4 in more detail, a number of different techniques are used with code to data comparisons, the preferred technique when an adequate basis of data exists. Code to code comparisons, model to model comparisons and engineering judgement are also important techniques.

The identification of important trends in the supporting experimental data and in the expected plant behaviour is an important step for several reasons. It allows analysts to select the proper models and codes to be used for a particular analysis and to evaluate the overall performance of the computer codes being used. It also provides an important check on the applicability of the computer codes or models to the type of transient or, in some cases, the reactor design being analysed. Although the documentation of the codes needs to provide some description of the limits of applicability of the codes, such descriptions provide only rough guidelines to the analyst.

The estimation of the uncertainties arising from the numerical approaches used in each code serves a number of primary needs. The uncertainties associated with the numerics of individual codes or models can arise from several sources. First, since many of the processes being modelled are non-linear, uncertainties can arise from the discretization of the equations used. Sensitivities to time step and nodalization are prime examples. Second, uncertainties can arise from differences in computer architecture, operating systems and compilers due to differences in machine accuracy, errors introduced by optimization of the compiler and installation errors.

Although many code developers assess the numerical accuracy of their codes for different machines, and provide guidelines on time step and nodalization, it is impossible for developers to evaluate all possible computer configurations for a complete range of code applications. From the perspective of code developers, the estimation of these uncertainties is important to ensure that the contributions from

the numerical approaches used are negligibly small compared with the overall modelling uncertainties, and that convergence in terms of time steps and nodalization can be obtained. From the perspective of analysts, this estimation is important to ensure that the proper user guidelines for such parameters as time step control and nodalization are followed and are appropriate to the problems being analysed. It is also important to ensure that the codes have been installed properly and that the influence of operating system errors and compiler errors on their computers has been minimized. As a consequence, it is important that analysts evaluate the impact of these uncertainties through convergence studies and comparison with developer supplied test problems.

The estimation of model uncertainties and code uncertainties, as discussed in more detail in Section 4, has been formalized using a range of methods. Fundamental to all methods is the adequacy of the supporting experimental data and the scalability of that basis of data to full plant conditions. The experimental data can be used in a variety of ways, with direct comparisons between the results of measurements and those of calculations being one of the most common approaches. Code to code comparisons, particularly the benchmarking of parametric codes and models against more mechanistic codes, are also important checks on the overall uncertainties in the codes. Assessment of codes with respect to fundamental problems, for which analytical solutions or other independent sources of results are available, is also valuable.

The estimation of uncertainties in the model or the code needs also to include the effects of important model input parameters. Although defaults for model input parameters have to be set by code developers to reflect the central or best estimate value of the uncertainty bands, this is not always done. In particular, in some parametric codes the model input parameters can be varied for each code to data or code to code comparison to minimize the variations in such comparisons. In this case analysts need to be aware of the influence of these parameters and to set them to reflect best estimate values on the basis of their own code to data or code to code comparisons appropriate to their applications. Recent efforts to automate the generation of uncertainty estimates through options such as the propagation of errors in the calculated results may help analysts. Sensitivity studies, particularly for the analysis of the later stages of severe accidents, can also be useful in gaining an understanding of the influence of important modelling parameters.

Code developers need to provide users with some guidance on usage, including nodalization guidelines, recommended modelling parameters, and estimates of the overall trends and uncertainties in typical code calculations. However, it is also important for analysts to assess the applicability of the codes for their particular application, to establish an adequate level of nodalization, to determine the impact of important modelling parameters, and to assess the trends and accuracy of the calculations in relation to their applications.

# 7. USER EFFECTS ON THE ANALYSIS

## 7.1. SOURCES OF USER EFFECTS

Although there has been substantial progress over the past two decades in the development of more accurate and more user tolerant computer codes for accident analysis, the user can still have a significant influence on the quality of the analysis. For example, as noted in a recent report by the OECD [44], the influence of the user on calculations for thermohydraulic codes for transient systems is still a subject of debate. This is most evident in the relatively wide variation in results from different organizations and code users participating in international standard problem (ISP) exercises. Although some of the user to user variation is due in part to the use of different computer codes, a substantial variation is also observed when different users employ the same codes.

Although the level of experience of the user, the type of code being used and the complexity of the system being analysed clearly have a strong influence on the results of the analysis, the OECD report identified several fundamental reasons why the user has such a strong influence on system thermohydraulic calculations. These include lack of adequate user guidelines and training, inadequate quality assurance processes to ensure that the input accurately reflects the system being analysed and limitations in the codes themselves. For example, the user has to make many input decisions for typical system code calculations, including: the level of system nodalization; input parameters for code models and specific system characteristics and components; initial and boundary conditions for the system; and, in some cases, state and transport properties. In addition, the input necessary for the system codes is extensive, needing in many cases thousands of input values. As a result, input errors are possible.

The reduction in user effects is currently being addressed in a number of ways; however, as noted in the following suggestions, more needs to be done. Firstly, the codes are being improved to help eliminate code input errors through more extensive checking and diagnosis for input errors. For example, the input processors now scan the input, identify probable input errors and warn the user if the values of the input parameters fall outside the ranges expected. More user friendly graphics–user interfaces are being developed that will help users to build and edit input files, display the results of system calculations in animated and other more intuitive ways, and provide direct comparisons with reference calculations or data. In addition, as part of the code development, the number of code options to be selected by code users is also reduced by more sophisticated modelling of the process. Secondly, code reference and input manuals are starting to take advantage of more advanced ‘desktop publishing’ and ‘hypertext’ techniques so that more extensive user guidelines can be

prepared and users can more readily access that information. For example, nearly all of the codes sponsored by the USNRC are now exclusively stored in electronic format with online help becoming more prevalent. Thirdly, new user training programmes are being developed to provide a more systematic way of training new or inexperienced code users and to provide for more enhanced technical exchanges between experienced users. This is certainly advantageous for widely used computer codes with high numbers of users.

## 7.2. REDUCTION OF USER EFFECTS

### 7.2.1. Qualification and training of users

User effects on the quality of the results of analysis can be reduced by systematic training. Even more important is the use of systematic training to ensure that software users are qualified to perform safety related analyses. Although the training necessarily depends to some extent on the type and end use of the results of the analysis, certain minimum conditions need to be satisfied to ensure that users can be effective analysts. Firstly, analysts performing safety related analyses need to have at least a basic understanding of the important phenomena and of methods of analysis, in particular reactor physics, thermohydraulics and fuel behaviour. Secondly, analysts need to have a basic understanding of the plant and its performance. The depth of understanding necessary on the part of the analyst in both cases depends strongly on the type of analysis being performed, the extent of supervision by more experienced staff and the overall knowledge of staff members available to support analytical activities. In general terms, strong supervision, teamwork, careful review and a good overall quality assurance programme (with associated standard practices and guidelines) can partially compensate for the limitations of individual analysts.

A prime factor contributing to efficient training and to achieving reliable results from a safety study is that the user belongs to a safety analysis group in charge of the methods and related applications for safety studies. In this framework, newer users can perform sensitivity calculations, whereas more experienced users can check the list of the key physical phenomena for an accident. Additionally, training of analysts can be performed as part of an overall formal training programme established by the organization responsible for the analysis. Such a training programme needs to include formal training plans with objectives and milestones, success criteria and written records of training activities. The training itself may consist of lectures prepared by more experienced analysts, reading assignments, participation in external courses and workshops, performance of relevant calculations and, most importantly, apprenticeships with more experienced analysts.

Although there are many different ways of classifying the specific training necessary for effective analysis, four fundamental types of training are suggested:

(a) University studies or other comparable courses in the phenomena important for analysis,
(b) Practical training on the design and operation of plants,
(c) Training specific to the software for the analysis,
(d) Application specific training.

Training on the phenomena is the most basic level of training and is, in many cases, provided at university level. University courses in thermohydraulics, heat transfer, structural analysis and/or reactor physics form the basis for design analysis or the analysis of normal plant operation and DBAs. Unfortunately, university courses on severe accident phenomenology and methods are much less widely available. As a result, training for severe accident analysis may be much more difficult to obtain. An effective severe accident analyst may need additional training in:

(1) Behaviour of fuel and other core materials, including the metallurgy of reactor core materials, material interactions and other chemical interactions, and the release of fission products;
(2) Combustion phenomena;
(3) Aerosol physics;
(4) More specialized thermohydraulics such as that for steam explosions.

In addition, severe accident analysis may necessitate some knowledge of probability theory and other methods used in PSA.

Practical training in the design and operation of the plant is also important for the effective analysis of DBAs and BDBAs. Table II gives an example of the relationship between the type of activity and the respective level of experience required. In Table II, activities identified as research and training denote the analysis of experimental facilities, the validation of individual code models through code to data and sensitivity studies on the basis of existing results of analysis. Analysis of plant accidents denotes the use of analytical software for plant calculations using pre-existing plant models. Development of plant models denotes the development of the plant system input models for the software.

It should be noted that cumulative experience may be built up through the total knowledge of the analysis group, embodying individual staff experience, rigorous documentation and the development of analytical procedures and guidelines (methods). This enables a reliable safety analysis to be performed by the group, while minimizing the influence of the actual number of years of experience of individual staff members. The cumulative experience may also come from outside the group

TABLE II. EXAMPLES OF ACTIVITIES AND EXPERIENCE REQUIRED OF ANALYSTS

| Activity | Experience |
|---|---|
| Research/analyst training | <3 years (phenomenological training assumed) |
| Analysis of plant accidents | 3–5 years |
| Development of plant models | 5–10 years |

through the use of consultants with suitable experience, in combination with rigorous training and the development of procedures and guidelines for use by group members.

Specific training in the use of the analysis software is usually provided by the software developer or certified trainer or optionally by other experienced users within the analysis group. Such training is important for an analyst to be able to use individual software packages effectively. The type of training necessary depends on the specific software being used but would cover, as a minimum, a review of the modelling concepts used in the software, validation of the software and application of the software to problems comparable with those the analyst is expected to encounter. In the case of software for analysis of severe accidents, a review of the important severe accident phenomena and the experimental data is probably appropriate because of the wide diversity of possible accident phenomena and the relative lack of other training specific to severe accidents.

Application specific training will typically be provided by the analyst's organization, although it is possible that some training can be provided by software developers or external bodies for generic classes of applications. Training in this area is most effective within the framework of a strong group of experienced analysts in combination with careful supervision and review. In the absence of a strong support group, participation in external software user groups and other technology exchange groups to discuss experience and problems is essential. In addition, such participation is important for the group as a whole to maintain an awareness of good practices in other organizations.

Analysts need to be encouraged during training at all levels to use independent tools and to make 'hand' calculations and other types of engineering calculations to check their analysis, whenever possible. Examples include the use of steady state mass and energy balances and the review of similar calculations. Integrated graphics–user interfaces which animate the results of analyses are also valuable tools which can be used to identify discontinuities, inconsistencies and in some cases numerical instabilities. Where possible, relevant experimental results could be used to benchmark the results of the analysis.

Formal qualification of analysts or of analyst training programmes is a more controversial goal, although it would be valuable in promoting a higher level of effectiveness on the part of the analyst and in helping to ensure the continued improvement of training methods. Unfortunately, because of the diversity of applications, development of a set of standards that could be used on a national or international basis would seem to be unlikely.

### 7.2.2. Method of analysis

The result of a safety analysis performed with a code depends strongly on the way the code is used; i.e. on the associated method. The availability of a method, in particular for the best estimate approach, permits a rigorous process for performing safety analyses. A method is typically defined for a given type of accident (e.g. main steam line break or LOCA) and for specified criteria (e.g. departure from nucleate boiling ratio or peak cladding temperature).

The method for a DBA analysis typically includes the following components (refer to Sections 4–6 for further details):

(a) Identification of the key physical phenomena. This is achieved through experimental analysis, simulations of transients or a review of comparable studies.
(b) Demonstration of the adequacy of the code. The demonstration is based on the code documentation. Specific code improvements and qualifications may be necessary. This step includes the choice of an appropriate nodalization. An evaluation matrix (a listing of the tests covering all the dominant phenomena and with which the code is compared) needs to be developed.
(c) Identification of the key parameters of the calculation. The key parameters of the calculation are the parameters which represent the dominant physical features: they can be initial conditions, boundary conditions, models and correlations. Their identification relies on experimental analysis and simulations of transients (sensitivity studies).
(d) Quantification of uncertainties (in line with Section 4).
(e) Reflection of uncertainties in the results. There are many possibilities to take account of these uncertainties. The first option is to bound each individual uncertainty. A more sophisticated way is a statistical combination of the results after the estimation of the individual uncertainties. Intermediate approaches (partially bounding and partially statistical) can be used.

A rigorous specification of the method seems to be an efficient way to control the effect of the user in safety analysis and to limit the risk of errors. A common

and precise formalism can be defined. The user, according to the previous sections, needs to do the following:

(1) To describe the assumptions of the accident study (initiator, criteria).
(2) To describe the accident transient using physical knowledge, on the basis of physical analysis and the results of research and development. For this step, comparison with available studies performed by equivalent codes can be useful.
(3) To justify the code capability to model or bound the major physical phenomena. Here the user relies on the description and qualification documentation of the code.
(4) To justify the adopted nodalization.
(5) To describe the chosen method.

A detailed knowledge of the phenomena occurring in an accident is needed for the development of methods, in order to take into account adequately the various physical contributions to the end result.

### 7.2.3. Other ways to reduce user effects

There are a number of other ways in which user effects can be further reduced. In general terms, the following activities are suggested. The user guidelines are not complete for many of the accident analysis codes and need to be improved. Systematic quality assurance procedures need to be used to qualify new sets of input data and to certify the use of previously developed sets for new applications. Code improvements also need to continue to address these concerns through the elimination of unnecessary input options, improved user interfaces and expanded checking of input errors. More extensive user instruction and training needs to be provided. Software users need to participate in software user groups and other technical exchange programmes associated with the validation and application of the software.

(a) Improved user guidelines. Although not a substitute for experience, improved user guidelines are necessary for new users. The detailed guidelines need to be code specific and also to reflect the possibilities of the organization in terms of hardware, software and personnel. In addition, these guidelines help to provide a mechanism to transfer knowledge from experienced users and code developers to new users.
(b) Continued improvement in codes. Improved checking for input errors and development of more advanced graphics–user interfaces will continue to reduce potential user errors.

(c) Independent validation of safety studies by each organization. It is essential for the training of the code user that independent validation of each specific code is performed by each organization. This validation can be based on a reasonably limited number of experiments taken from the whole validation matrix available and properly selected from three categories of experimental data:
  (i) Partial experiments related to the specific phenomena or a specific component.
  (ii) Integral experiments performed on a dedicated experimental facility.
  (iii) Real plant transient data. The selection of experimental data needs to reflect the characteristics of the particular reactor design.

(d) Independent checking and/or peer review of input decks. This is a powerful way of finding user errors. Critical calculations need to be performed by two individuals (or teams) acting independently. Independent checks using a different computer code on the same problem can also be effective. This can include duplicate calculations by the same organizations or, if the plants and conditions are similar, can include a review of similar calculations made by other organizations.

(e) Systematic user training. Responsibility is assigned to the code user to provide an adequate representation of the facility, to have adequate knowledge of important phenomena, and to be knowledgeable about the strengths and limitations of the individual codes. Although international standard problem exercises serve as training material for new users through exposure to relevant experiments and to more experienced users, systematic training and possibly user certification programmes for many of the codes need to be supported. This will be increasingly important as remaining experimental programmes are completed. In the past, many thermohydraulic systems analysts gained experience on codes through the analysis of large scale integral experiments such as the Loss of Fluid Test Facility in the USA. This experience was invaluable when these same codes were applied to the analysis of commercial power plants.

(f) Participation in software user groups and other technical exchange programmes. Participation in groups with other users not only ensures that a group of users is better informed about best available practices but also promotes improvement in those practices on a wider basis. Technical exchanges between experimentalists, model developers and other researchers involved in resolving important technical issues relating to a user's analytical work are effective ways of obtaining a greater breadth of experience and training. In particular, for severe accident analysis, for which active experimental and other research programmes are still in progress, such technical exchanges may be the only effective way of learning about important phenomena and methods of analysis.

# 8. PREPARATION OF INPUT DATA

## 8.1. COLLECTION OF PLANT DATA

The first important step in developing input data for the computer code for the plant under consideration is to collect the necessary documentation and other reliable sources of data; see also Annex I. The sources that serve as a basis for data collection may be as follows:

(a) Documentation on plant design;
(b) Technical specifications of equipment;
(c) Documentation gathered during the startup and commissioning of the installation;
(d) Operational documentation for the plant (limits and conditions, operating instructions, and records of operational regimes);
(e) 'As built' plant documentation.

All documents and other data sources used for the preparation of the input data need to be clearly identified and referenced.

If there is found to be a contradiction between the sources of information, this contradiction needs to be checked against a different independent source. An effective way to resolve a contradiction is to hold direct discussions with the operating organization. If documentation and/or data are missing or questionable, it is suggested that a walkdown of the plant be performed.

For the clarification of contradictory information, a comparison of data from plant to plant could also be carried out if the plants are similar (of the same type or of the same series) and if they were developed by the same general designer and equipment manufacturer. Such a comparison would need to be performed carefully owing to the fact that 'sister plants' cannot be guaranteed to be identical. In certain cases, if the missing data were replaced by truly plant specific data, the results of a comparison could be misleading.

All data necessary for the preparation of a particular computer code input deck can be compiled and formalized into a single specific document, called a 'database for safety analysis'. This database needs to contain all necessary information, such as information on geometry, thermal and hydraulic parameters, material properties, characteristics of the control system and set points, and the range of uncertainties in plant instrumentation devices, including drawings and other graphical documents (Annex III). It would preferably be independent of the type of analysis and the computer code used. The database is subject to quality control, and relevant quality assurance procedures need to be applied.

## 8.2. ENGINEERING HANDBOOK AND INPUT DECK

The creation of a plant model for computer codes is an interactive procedure that includes the selection of a nodalization scheme and preparation of the code input deck, and documentation of these activities. Depending on the objectives of the analysis, the plant model, or the code input deck, could be accident dependent.

The engineering handbook needs to be developed in parallel with the development of the code input deck (Annex III). This handbook is a document containing a full description and records of how the database has been converted into an input deck for the particular computer code. The document contains details of:

(a) Methods and simplifying assumptions used to convert the technical plant data into the code input data;
(b) All calculations made to convert the technical plant data to the necessary format for the input deck;
(c) Nodalization schemes used for a single component as well as for the complete system being modelled;
(d) All modelling assumptions made, adequately described and explained.

The engineering handbook needs to allow a unique interpretation of, and the reproducibility of, the code input. This handbook is subject to quality control and related quality assurance procedures for the ongoing maintenance of the contents.

The nodalization scheme of the modelled system needs to be established using the basic guidelines given in the code user's manual. This requires knowledge in depth of both the capabilities of the code and the specifics of the system modelled. Development of the nodalization scheme is typically an essential part of the preparation of the input data, since in most codes the quantification of the nodes plays an important part in the modelling of certain phenomena or specific effects in the system. However, refined nodalization does not always produce more precise analysis results. The adequacy of the nodalization needs to be confirmed by spatial convergence studies or on the basis of previous experience.

The final product of the preparation process for input data is the computer deck file for the input data, in the format needed by the code. It is advantageous to develop one 'master' input deck. Furthermore, it is strongly suggested that, before the final analysis is performed, the code version, the models selected by the user and the 'master' input deck be 'frozen' as they are and placed under strict control. Any necessary changes, once the analysis has begun, need to be peer reviewed and then approved and implemented by the individual responsible for the control. All changes needed for a specific calculation should to be recorded and documented so that the point at which improvements or corrections of errors have been introduced into the 'master' can be traced. Note that any changes to the code may necessitate

that the code be revalidated to show that it is still sufficiently accurate for the intended use.

## 8.3. VERIFICATION OF INPUT DATA

When the new input deck is being developed, errors could be introduced by a developer at any stage of the development process from the preparation of the engineering handbook to the preparation of the final input deck. Since these errors could result in unacceptable faults in the analysis, their early detection and correction are important.

Verification of the input deck is needed to check its formal correctness; i.e. that no erroneous data have been introduced into it and that all formal and functional requirements are fulfilled accurately and therefore will permit its successful use.

Current practice in accident analysis is to apply, in a systematic manner, the complete verification process. The verification process gives the confidence required that the modelling needs have been met. Verification of the input data involves reviewing and cross-checking the input deck and confirming that no mistakes have been made so that the input deck is ready for application. An effective way to avoid possible subjective errors in the development of the code input deck is to apply any available code specific preprocessing software.

The verification of the input deck needs to be performed and documented by qualified individuals or groups who have not been involved in the development of the input data. The reviewers can be from either the same organization or a different organization. They need to have access to all relevant documentation. All errors that were detected and corrections that were made in the verification process need to be properly documented.

## 8.4. VALIDATION OF INPUT DATA

Validation is performed after the verified input deck is completed and before the accident analysis is started. The purpose of validating input data is to demonstrate that the model adequately represents the functions of the modelled systems. Experience gained in the validation of the computer code and from the analysis of similar problems would be utilized in such a validation.

Validation of input data is an iterative process by means of which the correctness and adequacy of the plant models are confirmed so as to provide a good representation of the behaviour of the plant systems. The validation needs to assess whether the behaviour of the key performance parameters corresponds with reality. The validation would include, but not be limited to, the following:

(a) Checking the spatial and time convergence of the nodalization, for example, by performing a sensitivity analysis in relation to changes in nodalization for a typical case of the analysis under consideration.
(b) Checking the energy and mass balances in the systems modelled, including long term system energy and mass balances. This can be done by: comparing the power generation in the heated structures with the surface heat flux; comparing the power generation in individual components with the corresponding enthalpy rise; comparing the evaporation rate with the surface heat flux; comparing changes in mass inventories with the difference between the injection and leakage rates; checking the consistency of the flows in adjacent junctions.
(c) Checking the behaviour and response of individual components of the equipment or of the separate systems through determination of the respective boundary conditions.
(d) Checking the steady state conditions for different operational states, preferably by comparison with real plant data.
(e) Comparing the fluid volume and pressure distributions of the model with the height and pressure drops of the real installation.
(f) Performing a comparison between the NPP behaviour predicted by calculations with relevant data from measurements in integral test facilities.
(g) Checking the computational results against real plant data from operational events.

In relation to each of the aforementioned items, quantitative acceptance criteria for the code input deck could already be available or they could be established.

The plant data collected during commissioning and startup tests, conducted under well controlled conditions and with additional instrumentation, are very useful and need to be applied for validation of the input data. However, in some cases, such data may differ from the data obtained during plant operation. Consideration needs to be given to such differences where applicable.

For the validation process it is advisable to use tools for graphical display of the nodalization and simulation of the plant states.

# 9. PRESENTATION AND EVALUATION OF RESULTS

## 9.1. FORMAT AND STRUCTURE OF ACCIDENT ANALYSIS RESULTS

The results of an accident analysis need to be structured and presented in an appropriate format in such a way as to provide a good understanding and

interpretation of the course of the accident. A standardized format is suggested for similar analyses to facilitate interpretation and intercomparison of results.

Each case analysed needs to be clearly characterized by a description of its conditions, including:

- Definition of initiating events,
- Initial conditions of the system,
- Control system conditions and logic,
- Availability of systems and components,
- Method of analysis,
- Acceptance criteria.

Relevant references also need to be consulted.

The summary report of the accident analysis results needs to contain the following information:

(a) A chronology (timing) of the main events as calculated,
(b) A description and evaluation of the accident on the basis of the parameters selected,
(c) Figures showing plots of the main parameters calculated,
(d) A statement in relation to the fulfilment of the acceptance criteria,
(e) An evaluation of alternative scenarios (alternative conditions and sensitivity studies),
(f) References.

The structure and format need to be chosen in particular to permit easy checking of each individual acceptance criterion. The results of the analysis need to be presented and described in detail. They would consist of key parameters defining the status of the safety functions during the development of the process.

The presentation of the results needs to include a set of the important parameters in the course of a transient or accident as a function of time. This set needs to include all the parameters necessary to evaluate the status of the safety functions and the fulfilment of the acceptance criteria. It also needs to give information concerning the overall plant behaviour. Some of the parameters to be included in the lists are:

(1) Neutron power, decay heat and reactivity;
(2) Thermal power and heat fluxes in the active core;
(3) Minimal departure from nucleate boiling ratio or minimal critical power ratio (if relevant);
(4) Primary coolant conditions — temperatures, void fractions, flow and pressure;
(5) Maximal fuel temperatures;

(6) Maximal cladding temperatures;
(7) Reactor coolant inventory — total inventory and levels at key locations;
(8) Secondary system parameters showing heat flows;
(9) Containment pressure, temperature and the mass flow rate to the containment, if applicable;
(10) Activity of the release to containment and to the environment, if applicable;
(11) Hydrogen generation and distribution within containment;
(12) Level of core degradation, if applicable;
(13) Long term pressure buildup in the containment, if applicable;
(14) Parameters defining the performance of safety systems.

The presentation of the results needs to be sufficiently complete to allow the entire process to be displayed, starting from the initial steady state up to the long term safe stable condition. The presentation of accident analysis results needs to contain those parameters reflecting the key phenomena expected to occur in the course of the transient or accident.

The format and structure of the results needs to be chosen in such a manner as to show:

(i) The sequence of events and system operation in the course of the accident (from initial state to the final safe stable state);
(ii) Core and system performance;
(iii) Physical barrier performance;
(iv) Radiological consequences, if appropriate.

The format of the results needs to be such as to allow an intercomparison with the results obtained from the same or different codes. It is suggested that the presentation of the results be user friendly for purposes of easy understanding and interpretation. This needs to include development of graphically oriented displays.

## 9.2. REVIEW OF ACCIDENT ANALYSIS RESULTS

Before any use of the results, their correctness needs to be carefully checked, on the basis of user experience and logical judgement, comparison with similar calculations, sensitivity analysis and consistency with general findings. The results derived then need to be reviewed and evaluated in relation to the initial goal and purpose of the analysis, such as licensing, improvement of operational documentation or plant upgrading.

The prime objective of reviewing the results is to check by comparison of calculated values with criteria whether the acceptance criteria have or have not been satisfied.

If the analysis is used for the evaluation of the system safety performance, the review and discussion of the results needs to be focused on maintaining the safety functions and the status of the physical barriers.

A certain amount of attention needs to be devoted in the discussion of the results to their sensitivity to the key input parameters as well as to the expected uncertainties and the tolerance band of the parameters.

The review of the results should also lead to a specification of the additional analysis needed to achieve a complete understanding of the accident under consideration and the resolution of the relevant safety issue.

The review and discussion of the results need to address the correctness of the calculations. The correctness would be checked by comparing the results discussed with those obtained by alternative methods and/or codes or with those obtained using the same methods and/or codes for a similar plant.

## 10. QUALITY OF ACCIDENT ANALYSIS

Accident analysis needs to be the subject of a comprehensive quality assurance programme applied to all activities affecting the quality of the final results, in accordance with general international requirements [45]. The quality assurance programme needs to define the quality assurance standards to be applied in accordance with national requirements and internationally recognized good practices. Such a programme would consider the following general principles.

Formalized quality assurance procedures and/or instructions need to be developed and reviewed for the whole accident analysis process, including:

(a) Collection and verification of plant data,
(b) Verification of the computer input deck developed and documentation of detected errors,
(c) Validation of plant models.

It is helpful to approve a document on the method of analysis (see also Section 7.2.2) prior to performing an analysis. Such a document lists the models to be used, system assumptions, acceptance criteria and system nodalization: its review and approval by line management prior to doing the analysis reduces the risk of mistakes and subsequent redoing of the work.

The responsibilities of all individuals in the organization involved in the analyses need to be clearly specified. Safety analysts need to be trained and qualified, and their qualifications need to be adequately documented.

All documents, including calculational notes and results, need to be recorded to allow them to be independently checked by qualified reviewers. An effective control of non-conformance with procedures, as well as control of corrective actions, needs to be introduced. Validated and accepted methods and tools need to be used, and their uses need to be referenced and documented. All sources of data need to be clearly referenced and documented.

The results can be checked using one or more of the following techniques, depending on the importance of the analysis:

(1) Supervisory review,
(2) Peer review,
(3) Independent review by a competent individual,
(4) Independent calculation of the same case under analysis by a competent individual.

All differences found during the review need to be resolved to the satisfaction of the reviewer and/or line management before the final use of the results.

All safety analyses used for plant licensing need to be archived so that the code version, code documentation, input data and calculational results are recoverable.

# REFERENCES


[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standard Series No. NS-R-1, IAEA, Vienna (2000).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Legal and Governmental Infrastructure for Nuclear, Radiation, Radioactive Waste and Transport Safety, Safety Standards Series No. GS-R-1, IAEA, Vienna (2000).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Review and Assessment of Nuclear Facilities by the Regulatory Body, Safety Guide, Safety Standards Series No. GS-G-1.2, IAEA, Vienna (2002).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidelines for Accident Analysis of WWER Nuclear Power Plants, IAEA-EBP-WWER-01, Vienna (1995).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidelines on the Pressurized Thermal Shock Analysis for WWER Nuclear Power Plants, IAEA-EBP-WWER-08, Vienna (1997).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Anticipated Transients without Scram for WWER Reactors, IAEA-EBP-WWER-12, Vienna (1998).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidelines for WWER 440/213 Containment Evaluation, TC Project RER/9/005, IAEA-TA-7488, WWER-SC-170, Vienna (1996).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Analysis of Accidents in Shutdown Modes for WWER Nuclear Power Plants, IAEA-EBP-WWER-09, Vienna (1997).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Primary to Secondary Leaks in WWER Nuclear Power Plants, IAEA-EBP-WWER-13, Vienna (2000).

[11] US NUCLEAR REGULATORY COMMISSION, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition), Regulatory Guide 1.70, US Govt Printing Office, Washington, DC (1979).

[12] US NUCLEAR REGULATORY COMMISSION, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Rep. NUREG-0800, US Govt Printing Office, Washington, DC (1982).

[13] ATOMIC ENERGY CONTROL BOARD, Requirements for the Safety Analysis of CANDU Nuclear Power Plants, Consultative Document C-6, AECB, Ottawa (1980).

[14] ENERGOATOMIZDAT, General Regulations of Safety Insurance of Nuclear Power Plant Safety (OPB-88), Rep. PNAE G-1-011-89, Energoatomizdat, Moscow (1990) (in Russian, English translation available).

[15] ENERGOATOMIZDAT, Standard Format of Technical Substantiation of Nuclear Power Plant Safety (TS TOB AS-85), Rep. PNAE G-1-01-85, Energoatomizdat, Moscow (1987) (in Russian).

[16] ELECTRICITE DE FRANCE, FRAMATOME, Design and Construction Rules for System Design of 900 MW(e) PWR Nuclear Power Plants, Rep. Rule SIN 3130/84, Rev. 4, Ministère de l'Industrie et de la Recherche, Paris (1991).

[17] FEDERAL MINISTRY OF THE INTERIOR, Compilation of Information for Review Purposes under Licensing and Supervision Procedures for Nuclear Power Plants, Rep. RSK Guideline, BMI, Bonn (1982).
[18] RADIATION AND NUCLEAR SAFETY AUTHORITY FINLAND: STUK, Finnish Guide: Transient and Accident Analysis for Justification of Technical Solutions at Nuclear Power Plants, YVL-Guide 2.2, STUK, Helsinki (1987).
[19] INTERNATIONAL ATOMIC ENERGY AGENCY, The Safety of Nuclear Installations, Safety Series No. 110, IAEA, Vienna (1993).
[20] US NUCLEAR REGULATORY COMMISSION, Domestic Licensing of Production and Utilization Facilities, Code of Federal Regulations 10, Part 50, US Govt Printing Office, Washington, DC (1995).
[21] AMERICAN NATIONAL STANDARDS INSTITUTE, Revision and Addendum to Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants, Rep. ANSI-N18.2A-1995, ANSI, New York (1995).
[22] ATOMIC ENERGY CONTROL BOARD, Requirements for Containment Systems for CANDU Nuclear Power Plants, Regulatory Document R-7, AECB, Ottawa (1991).
[23] ATOMIC ENERGY CONTROL BOARD, Requirements for Shutdown Systems for CANDU Nuclear Power Plants, Regulatory Document R-8, AECB, Ottawa (1991).
[24] ATOMIC ENERGY CONTROL BOARD, Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants, Regulatory Document R-9, AECB, Ottawa (1991).
[25] US NUCLEAR REGULATORY COMMISSION, Domestic Licensing of Production and Utilization Facilities, Code of Federal Regulations 10, Part 50, US Govt Printing Office, Washington, DC (1974).
[26] COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS, CSNI Status Summary on Utilization of Best-Estimate Methodology in Safety Analysis and Licensing, Rep. NEA/CSNI/R (1996) 19, OECD Nuclear Energy Agency, Paris (1996).
[27] BERNA, G.A., et al., FRAPCON-2: A Computer Code for the Calculation of Steady State Thermal-Mechanical Behaviour of Oxide Fuel Rods, Rep. NUREG/CR-1845, US Govt Printing Office, Washington, DC (1981).
[28] SIEFKEN, L.J., et al., FRAPT-T6: A Computer Code for Transient Analysis of Oxide Fuel Rods, Rep. NUREG/CR-2148, EGG-2104, US Govt Printing Office, Washington, DC (1981).
[29] TESCHENDORF, V., et al., "Current and anticipated uses of thermal-hydraulic codes in Germany", paper presented at OECD/CSNI Workshop on Transient Thermal-Hydraulic and Neutronic Codes, Annapolis, 1996.
[30] ALLISON, C.M., MILLER, C.S., WADE, N.L. (Eds), RELAP5/MOD3 Code Manual (Vols 1–4), Rep. NUREG/CR-5535, US Govt Printing Office, Washington, DC (1995).
[31] TRAMBAUER, K., "The Code ATHLET-CD for the simulation of severe accidents in light water reactors", paper presented at 5th Int. Top. Mtg on Nuclear Reactor Thermal Hydraulics, Salt Lake City, 1992.
[32] BARRE, F., et al., "New developments in the CATHARE 2 code", paper presented at 6th Int. Top. Mtg on Nuclear Reactor Thermal Hydraulics, Grenoble, 1993.

[33] SUMMERS, R.M., et al., MELCOR Computer Code Manuals, Primer and User's Guide, Rep. NUREG/CR-6119, SAND93-2185, US Govt Printing Office, Washington, DC (1994).
[34] HANNA, B.N., "CATHENA: A thermohydraulic code for CANDU analysis", Nucl. Eng. Des. **180** (1997) 113.
[35] BOYACK, R., et al., Quantifying Reactor Safety Margins: Application of Code Scaling, Applicability, and Uncertainty Evaluation Methodology to a Large-Break, Loss-of-Coolant Accident, Rep. NUREG/CR-5249, EGG-2552, US Govt Printing Office, Washington, DC (1989).
[36] ORTIZ, M.G., GHAN, L.S., Uncertainty Analysis of Minimum Vessel Liquid Inventory during a Small Break LOCA in a B&W Plant: An application of the CSAU Methodology Using the RELAP5/MOD3 Computer Code, Rep. NUREG/CR-5818, EGG-2665, US Govt Printing Office, Washington, DC (1992).
[37] ALMEIDA, C., "Best estimate approach for accident analysis of nuclear power plants", paper presented at IAEA Workshop on Code Validation and Uncertainties Evaluation, Trnava, 1996.
[38] US NUCLEAR REGULATORY COMMISSION, Best Estimate Calculations of Emergency Core Cooling System Performance, Regulatory Guide 1.157, US Govt Printing Office, Washington, DC (1989).
[39] BIBILASHVILI, Y., paper presented at the IAEA Consultants Mtg on Fuel Safety Criteria, Vienna, 1998.
[40] US NUCLEAR REGULATORY COMMISSION, SCDAP/RELAP5/MOD3.1 Code Manual, Vols 1–5, Rep. NUREG/CR-6150, US Govt Printing Office, Washington, DC (1985).
[41] GONZALEZ, R., FICHOT, F., CHATELARD, P., "Status of ICAR2 and ICARE/CATHARE development", paper presented at the Winter ANS Meeting, Washington, DC, 1996.
[42] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety Series No. 50-P-4, IAEA, Vienna (1992).
[43] BROCKMEIER, U., et al., In-Vessel Core Degradation in LWR Severe Accidents: A State of the Art Report, Update January 1991–June 1995, AEA/CSR 1025/W, AEA Technology, Culham (1995).
[44] GLAESER, H., "User effects in application of thermal-hydraulic computer codes", paper presented at IAEA Specialists Mtg on User Qualification for and User Effect on Accident Analysis for NPPs, Vienna, 1998.
[45] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations, Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

# LIST OF ABBREVIATIONS

| | |
|---|---|
| AECB | Atomic Energy Control Board (Canada) |
| ASDV | Atmospheric steam discharge valve |
| ATWS | Anticipated transients without scram |
| BDBA | Beyond design basis accident |
| BOL | Beginning of life |
| BWR | Boiling water reactor |
| CANDU | Canadian deuterium uranium (reactor) |
| CCF | Common cause failure |
| CFD | Computational fluid dynamic |
| CFR | Code of Federal Regulations (USA) |
| CSAU | Code scaling, applicability and uncertainty |
| CSDV | Condenser steam discharge valve |
| CSNI | Committee on the Safety of Nuclear Installations |
| DBA | Design basis accident |
| DNBR | Departure from nucleate boiling ratio |
| ECC | Emergency core cooling |
| ECCS | Emergency core cooling system |
| EOL | End of life |
| EOP | Emergency operating procedure |
| FMEA | Failure modes and effects analysis |
| FW | Feedwater |
| HFP | Hot full power |
| HTS | Heat transport system |
| HZP | Hot zero power |
| I&C | Instrumentation and control |
| ICRP | International Commission on Radiological Protection |
| ISP | International standard problem |
| LB | Large break |
| LOCA | Loss of coolant accident |
| LOECC | Loss of emergency core cooling |
| LOFA | Loss of flow accident |
| LOFT | Loss of fluid test |
| LRV | Liquid relief valve |
| MCP | Main circulation pump |
| MSSV | Main steam safety valve |
| NDT | Non-destructive testing |
| NEA | Nuclear Energy Agency (OECD) |
| NPP | Nuclear power plant |
| NUSS | Nuclear safety series |

| | |
|---|---|
| OECD | Organisation for Economic Co-operation and Development |
| PCT | Peak cladding temperature |
| PHWR | Pressurized heavy water reactor |
| PRZ | Pressurizer |
| PSA | Probabilistic safety analysis/assessment |
| PTS | Pressurized thermal shock |
| PWR | Pressurized water reactor |
| QA | Quality assurance |
| RBMK | High power boiling reactor with pressurized channels (Russian design) |
| RCS | Reactor coolant system |
| RHR | Residual heat removal |
| RIH | Reactor inlet header |
| ROH | Reactor outlet header |
| ROP | Regional overpower protection |
| RRS | Reactor regulating system |
| SB | Small break |
| SDS1 | Shutdown system No. 1 |
| SDS2 | Shutdown system No. 2 |
| SG | Steam generator |
| TMI | Three Mile Island (USA) |
| WWER | Water moderated, water cooled power reactor (Russian design) |

# DEFINITIONS

*These definitions were compiled solely for the purposes of the present report on Accident Analysis for Nuclear Power Plants. They do not represent a consensus or an endorsement by the IAEA.*

**acceptance criteria**. Quantitative limitation of selected parameters or qualitative requirements set-up for the results of accident analysis. Specified bounds on the value of a functional or condition indicator used to assess the ability of a system, structure or component to perform its design function.

**accident**. Any unintended event, including operating errors, equipment failures or other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety.

**accident analysis**. In its broad sense, as used in this Safety Report, the term is used for deterministic safety analysis of any of the anticipated operational occurrences, DBAs and BDBAs.

**accident conditions**. Deviations from normal operation more severe than anticipated operational occurrences, including DBAs and severe accidents.

**accident management**. The taking of a set of actions during the evolution of an event sequence to a BDBA:

— To prevent the escalation of the event into a severe accident (preventive accident anagement measures),
— To mitigate the consequences of a severe accident,
— To return the plant to a long term safe stable state.

**accident management programme (AMP)**. Plans and actions undertaken to ensure that the plant and its personnel with responsibilities for accident management are adequately prepared to take effective on-site actions to prevent or to mitigate the consequences of a severe accident.

**accuracy**. The known bias between a code prediction and the actual transient performance of a real facility.

**anticipated operational occurrence**. An operational process deviating from normal operation which is expected to occur once or several times during the operating lifetime of the power plant but which, in view of the appropriate design

provisions, does not cause any significant damage to items important to safety nor lead to accident conditions.

**anticipated transient without scram (ATWS)**. Accident for which the initiating event is an anticipated operational occurrence, but for which the reactor fast shutdown system fails.

**best estimate analysis**. Accident analysis which:

(1) Is free of deliberate pessimism regarding selected acceptance criteria,
(2) Uses a best estimate code,
(3) Includes an uncertainty analysis.

**best estimate code**. A code which:

(1) Is free of deliberate pessimism regarding selected acceptance criteria,
(2) Contains a sufficiently detailed model to describe the relevant processes that require to be modelled.

**beyond design basis accident (BDBA)**. Accident conditions more severe than those of a DBA. An accident falling outside the plant and its safety systems design envelope. A BDBA *may or may not* involve core degradation.

**code validation**. Assessment of the accuracy of values predicted by the code against relevant experimental data for the important phenomena expected to occur.

**code verification**. Review of the source coding relative to its description in the documentation.

**common cause failure**. The failure of a number of devices or components to perform their functions as a result of a single specific event or cause.

**conservative**. Leading to pessimistic results relative to specified acceptance criterion/criteria.

**controlled safe state**. A plant state in which:

(1) The core is and remains subcritical.
(2) The core is in a coolable geometry and there is no further fuel failure.
(3) Heat is being removed by the appropriate heat removal systems.
(4) Fission product releases from containment have ceased, or further releases can be bounded.

**core damage**. Substantial loss of the core geometry with major radioactive release, leading to conditions beyond the criteria established for DBAs, typically due to excessive core overheating.

**core damage frequency**. Expected frequency of occurrence (usually expressed in reactor-years$^{-1}$) of an event leading to core damage, as calculated in a Level 1 PSA.

**core degradation**. A process that leads to core damage.

**design basis accident (DBA)**. Accident conditions against which an NPP is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

**deterministic safety analysis**. Analysis using, for key parameters, single numerical values (taken to have a probability of 1), leading to a single value of the result. This safety analysis is performed under specific predetermined assumptions concerning the initial operational state and the initiating event, with specific sets of rules and acceptance criteria. Deterministic analyses can be conservative or best estimate.

**emergency operating procedures (EOPs)**. A set of documents describing the detailed actions to be taken by response personnel during an emergency. The plant specific procedures contain instructions to operating staff for implementing preventive accident management measures, for both DBAs and BDBAs.

**input data validation**. Confirmation of the correctness and adequacy of the plant models in providing a good representation of the actual behaviour of the plant systems.

**input data verification**. Independent reviewing and cross-checking of the input deck and confirming that no mistakes have been made and that the input deck is ready for application.

**mechanistic BDBA code**. A code which includes the best estimate phenomenological models necessary to provide an accurate prediction of the behaviour of an NPP. The modelling uncertainties of the code should be comparable to the uncertainties in the data used to validate the code. User defined modelling parameters should be eliminated as far as practicable.

**normal operation**. Operation of an NPP within specified operational limits and conditions including startup, power operation, shutting down, shutdown, maintenance, testing and refuelling.

**operational limits and conditions**. A set of rules setting forth parameter limits that ensure the functional capability and the performance levels of equipment for safe operation of an NPP, approved by the regulatory body.

**operational states**. States defined under normal operation or anticipated operational occurrences.

**parametric BDBA code**. A code which includes a combination of phenomenological and user defined parametric models necessary to describe the important trends in behaviour of an NPP. Extensive user defined modelling parameters to allow the user to bound important processes or phenomena.

**postulated initiating events**. An event identified during design as capable of leading to anticipated operational occurrences or accident conditions.

**power excursion**. Uncontrolled change, typically an increase, of the reactor fission power.

**probabilistic safety assessment (PSA)**. A comprehensive structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk. Three levels of PSA are generally recognized. Level 1 comprises the assessment of plant failures leading to the determination of core damage frequency. Level 2 includes the assessment of containment response leading, together with Level 1 results, to the determination of containment release frequencies. Level 3 includes the assessment of off-site consequences leading, together with the results of Level 2 analysis, to estimates of risks to the public.

**protection system**. A system which monitors the operation of a reactor, which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition.

**safety analysis**. An analytical study, usually performed by means of computer codes, by which it is demonstrated how safety requirements are met.

**safety function**. A specific purpose that must be accomplished for safety.

**safety margin (absolute terms)**. Difference, in physical units, between the critical value of an assigned parameter associated with the failure of a system or a component, or with a phenomenon, and the actual value of that parameter.

**safety margin (in consideration of the results of analyses)**. The difference, in physical units, between a threshold that characterizes an acceptance criterion and the result provided by either a best estimate calculation or a conservative calculation. In the case of a best estimate calculation, the uncertainty band must be used when defining the safety margin.

**safety systems**. Systems important to safety provided to assure safe shutdown of a reactor or residual heat removal from a core, or to limit the consequences of anticipated operational occurrences and DBAs.

**sensitivity analysis**. A quantitative examination of how the behaviour of a system varies with changes, usually in the values of the governing parameters. Systematic variation in code input variables or modelling parameters to determine the influence of physical phenomena and/or of code input variables on the overall analysis results.

**severe accident**. An accident more severe than a DBA and involving significant core degradation.

**severe accident conditions**. See severe accident.

**severe accident management (SAM)**. A subset of accident management measures that:

— Terminate core damage once it has started,
— Maintain the capability of the containment as long as is possible,
— Minimize on-site and off-site releases,
— Return the plant to a controlled safe state.

**severe accident management guidelines (SAMGs)**. A set of guidelines containing instructions for actions in the framework of severe accident management.

**single failure**. A random failure which results in the loss of capability of a component to perform its intended safety function. Consequential failures resulting from a single random occurrence are considered to be part of the single failure. For PHWRs, a single failure is the failure of a process system.

**system code**. A computer model that is capable of simulating the transient performance of a complex system like an NPP. A system code typically includes equations for thermohydraulics, neutronics and heat transfer and must be equipped with special models to simulate the performance of components such as pumps and separators. The code should typically also simulate the control logic implemented in the plant and be able to predict the accident evolution.

**uncertainty analysis**. An analysis to estimate the uncertainties and error bounds of the quantities involved in, and the results from, the solution of a problem. Estimation of individual modelling or overall code uncertainties, representation uncertainties, numerical inadequacies, user effects, computer/compiler effects and plant data uncertainties for the analysis of an individual event.

## Annex I

## PROCEDURE FOR PERFORMING AN ACCIDENT ANALYSIS

Performing an accident analysis is a complex task, which places significant requirements on analysts. These requirements usually include knowledge of the dominant physical phenomena and associated computer code(s) used in the analysis, knowledge of the plant analysed and knowledge of the relevant legislation which is in force in the field of reactor safety in a given country. Accident analysis is performed in several steps. These steps need not always be sequential; some can be carried out in parallel. Different kinds of activities are performed within each step. A general flow chart illustrating this procedure is shown in Fig. I–1. Details for the activities indicated in the flow chart have already been given in the main text. The main activities are briefly summarized below.

**Specification of the facility and objectives of the accident analysis**. Before starting an accident analysis the facility (e.g., which unit of an NPP) that is to be analysed needs to be clearly specified. For an NPP with several units, one reference unit is typically selected. Clear definition of the goals and scope of the accident analysis are prerequisites for successful performance of the accident analysis.

**Selection of the approach to be used**. The approach to be applied for different purposes and for design and licensing (level of conservatism) depends in particular on the national regulatory requirements and needs to be defined or agreed with the final user of the results. The national nuclear regulatory body is typically involved. The approach needs to clearly define the kind of computer codes that may be used in the accident analysis and how the necessary level of conservatism needs to be reached (e.g., a combination of best estimate codes with pessimistic assumptions or, in addition, with an estimation of the uncertainties in an analysis).

**Selection of a computer code**. For all applications, use of best estimate computer codes is suggested, preferably internationally recognized ones. Several computer codes are often used consecutively for more complex applications. Validation of the codes for intended applications is an essential precondition for their selection. It is always useful to agree on the selection of the code with the final user of the results and/or with the regulatory body.

**Methodology of the accident analysis**. The goal of analysts simulating the transient performed on an experimental facility is to obtain results which agree well with the experimental data. The main purpose of accident analysis for a real unit is

usually to demonstrate that the safety goals are met. In the licensing analysis these goals are transformed into the form of acceptance criteria. Depending on the probability of the analysed event, the fulfilment of the acceptance criteria usually needs to be demonstrated by using some kind of conservative or best estimate approach or a combination of both. In general, for events with higher probability of occurrence, more stringent assumptions need to be applied in accordance with regulatory requirements. Unlike the analysis of transients performed on experimental facilities with exactly defined initial and boundary conditions, an important part of the accident analysis of real NPPs is the selection of initial and boundary conditions, corresponding to given acceptance criteria. The choice of acceptance criteria affects substantially the assumptions of the analysis: in general different acceptance criteria necessitate different sets of assumptions. The selection of conservative initial conditions needs to be based upon specified confidence limits for the uncertainties of those parameters. For conservative analysis, the selection of the availability of plant systems and components (the boundary conditions) is typically based upon the single failure criterion. The functioning of control systems is considered only if their operation has a negative impact on the course of an accident. It is usually assumed that operator action does not take place in the prescribed time period, but that after this the action is successful in accordance with existing EOPs. The method of accident analysis may also include quantification of uncertainties. Further details about methods are provided in Section 7.2.2.

**Collection of the plant data.** 'As designed' and/or 'as built' documentation as well as operational documentation for the unit under consideration needs to be collected, checked and referenced. These data are necessary for preparation of the database. In addition to these data, operational records (e.g. records of transients or incidents that occur during plant operation and records of startup experiments) may be very valuable in the process of input data deck validation.

**Database for the accident analysis**. The starting point in the development of the plant specific input data deck ('plant model') is the plant database. The plant model has to be prepared using reliable plant data. The reason for the development of the database for accident analysis is to collect, formalize and reference in appropriate form all the data which are necessary in accident analysis. The scope of the database depends on the intended field of applications (e.g. anticipated transients, DBAs, severe accidents, analysis of primary and secondary systems and analysis of confinement). In the processes of the preparation and updating of the database, close co-operation with technical staff from the NPP is necessary. It is practical to develop the database in code independent form. This can be done quite easily in the field of thermohydraulic analysis of DBAs; for example, the input data necessary for most system transient analysis codes are nearly the same. In Fig. I–1

the requirements on the database that depend on code selection are indicated with dashed lines.

**Engineering handbook**. An engineering handbook represents an intermediate step between the database and the input data deck. A full description of how the plant data have been converted into an input data deck for a given computer code needs to be presented in this document. The database and the code user's manual are used for development. The engineering handbook should allow a unique interpretation and reproducibility of the code input data deck. It is strongly recommended that an independent review of the engineering handbook be performed.

**Development of the input data deck**. On the basis of the engineering handbook, an input data deck representing the reference plant needs to be developed. The final product is the file in the format required by the computer code. This file can be split into a general part describing the plant ('plant model') and a specific part describing the scenario of an accident. The plant model includes data describing the geometry, material properties, flow regimes, core kinetics, plant controllers and safety systems. It is obvious that even for complicated scenarios with a number of operator interventions the plant model represents the majority of the input data deck. Sufficiently versatile, validated and optimized (in terms of the stability and computational speed) the plant model is a powerful tool, which may reduce the effect of the user significantly. The basic recommendations from code manuals should be followed during the development of the plant model.

**Verification and validation of the input data deck**. The input data need to be verified and validated in order to provide confidence that the modelling requirements have been fully met and that the performance and functionality of the input deck are adequate. The verification process is part of quality control and related QA procedures. A plant model representing the reference plant can be considered verified and validated ('qualified') when the following conditions are met:

(a) It has geometrical and material fidelity with the reference system (e.g. all important flow paths are simulated).
(b) It reproduces properly all the important parameters measured in the reference NPP in steady state conditions.
(c) Sufficient agreement is reached in the transient conditions available.

The standard procedures for the qualification of a developed input data deck usually consist of 'steady state' and 'on-transient' level qualifications. A list of representative parameters should be used for assessment of the plant model in steady state conditions. The data from transients recorded in the units operated may be very

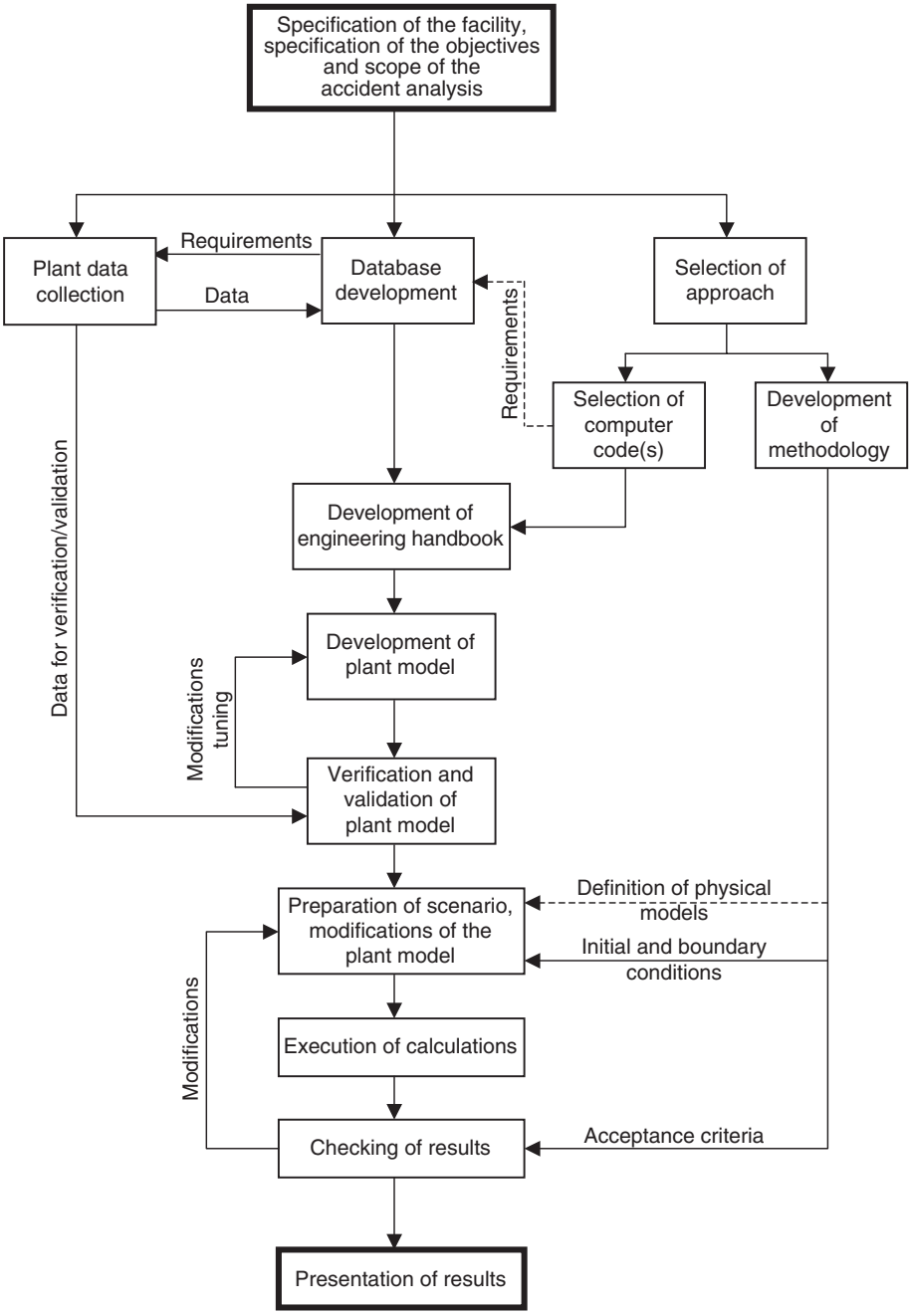



*FIG. I–1. Flowchart of the basic steps in the accident analysis procedure. The dashed lines indicate the requirements on the database that depend on code selection.*

valuable in the 'on-transient' level validation of the plant model. However, serious accidents are quite unlikely during operation of NPPs. Therefore only records of anticipated operational occurrences, covering a narrow range of parameters, are usually available. The records from the units operated are useful, especially for tuning of the plant model: checking heat losses, heat capacities, pressure losses, response of plant controllers, discharge capacities of relief and safety valves, and pump characteristics.

**Preparation of the scenario**. The scenario for the accident needs to be prepared after the verification process has been completed. Initial and boundary conditions need to be set in accordance with the methodology of the accident analysis. Input data for the definition of an initiating event (e.g. break size and location) should be prepared. A choice from various optional code models (e.g. break flow model, heat transfer correlations) needs to be made. Default options are recommended if specific models are not available.

**Execution of the calculation**. The calculation of the accident according to code requirements is performed resulting in code output documents.

**Checking of the results**. Once the calculation has been completed, the results need to be checked through one or more of the following: supervisory review, independent calculations, comparison with a similar analysis, peer review and spot checking calculations for internal consistency. If necessary, corrections should be made to the input data deck and the calculation should be repeated. The limiting values of key parameters need to be estimated in order to check whether the acceptance criteria are met.

**Presentation of the results**. The results of the accident analysis need to be structured and presented in an appropriate way to provide a good understanding and interpretation of the course of the accident. Advanced software tools enabling complex visualization of the course of the accident are recommended. Each case analysed needs to be clearly characterized by a description of the conditions and representative parameters of the process. An appropriate structure and format of the presentation should be chosen to permit easy checking of each individual acceptance criterion. In addition to other data, the results should include a set of key parameters as a function of the time needed to evaluate the status of the safety functions and the physical protective barriers. Finally, the presentation of the results needs to include conclusions concerning the achievement of the primary goals of the analysis.

## Annex II

## UNCERTAINTY ANALYSIS FOR DESIGN BASIS ACCIDENTS WITH BEST ESTIMATE ANALYSIS CODES

### II–1. INTRODUCTION

This annex describes the increasing importance of uncertainty analysis, as the use of best estimate codes becomes more widespread. The types of uncertainty — in the computer models, in the simulation of the plant and in the plant parameters themselves — are listed. A number of techniques for uncertainty analysis that are currently in use in various countries are summarized. Since these analyses tend to be resource and computer intensive, some pragmatic suggestions are made on where countries with modest capabilities can begin.

### II–2. NEED FOR UNCERTAINTY ANALYSIS

The main text of this Safety Report has indicated a preference for the use of best estimate codes in safety analyses; i.e. codes which represent the physical phenomena as accurately as possible without a deliberate bias. In fact, codes such as reactor physics codes have always been used as 'best estimate' tools; it is the thermohydraulic codes in which the physical models have in some cases been deliberately biased in a pessimistic direction.

Licensing analysis has historically necessitated a pessimistic bias in the result. Where best estimate codes are used for licensing analysis, such a pessimistic bias may be achieved by the use of conservative input data, particularly for parameters to which the answer is known to be sensitive.

However, the degree of conservatism in the result is not quantifiable using this approach alone, owing to uncertainties in the ability of the best estimate codes to predict reactor conditions. Regulators reviewing licensing analysis usually want to know the margins between the results of accident analysis as presented and any abrupt changes for the worse in those results as conditions vary (the 'cliff edge' effect). To quantify these margins, uncertainty analysis is used. Uncertainty analysis is even more important if best estimate codes are used with best estimate data. Such a practice is not yet common for licensing analysis, although it is used in accident analyses in support of PSAs.

There are also varying degrees of pessimism about the data. When best estimate codes are used for licensing analysis, the input data and plant assumptions

are usually highly pessimistic in order to provide assurance that all possible values and plant conditions have been bounded. This approach can lead to a number of problems [II–1]:

(a) The predictions of the computer codes can be so severe that the physical conditions are in areas where no validation is possible (e.g. very high fuel temperatures).
(b) The margins to acceptance criteria may be very small, particularly for low frequency events.
(c) The small margins to acceptance criteria, or the violation of acceptance criteria if the data assumptions are very conservative, may lead to unnecessary economic penalties owing to restricted regimes of plant operation.
(d) If the input data describing the plant are indeed chosen to bound all possible regimes of plant operation, undue emphasis is given to low probability plant states at the limit of the operating envelope.

Excessive conservatism can also mask potential safety issues by failing to capture the relevant physical phenomena. For example, overprediction of containment pressure to determine the margins to the design pressure in a pessimistic way gives a non-conservative prediction of those signals which depend on containment pressure to initiate mitigating action. While this example is well known and easily countered, other effects may be more subtle; for example, if the coolant flow in normal operation is higher than that assumed in the accident analysis, this may be conservative for predicting the onset of fuel dryout but it is non-conservative for the timing of low flow trips and may mask high pressure trips.

There are some disadvantages to performing comprehensive uncertainty analyses. As noted earlier, the costs of analysis and regulatory review will increase, and the computing time necessary may be quite large. The regulatory body may also, for historical or traditional reasons, require certain deterministic practices to be retained — use of the single failure criterion in LWRs, or no credit for off-site power or credit for only one of two independent shutdown systems in CANDU — thereby introducing a pessimistic bias in plant performance predictions.

## II–3. USES OF UNCERTAINTY ANALYSIS

As noted in Section II–2 above, uncertainty analysis can quantify the uncertainty in safety margins and therefore provide confidence (or otherwise) that the margins are acceptable. This can assist regulatory decision making, especially for low probability events within the design basis.

When the uncertainty analysis is extended to include plant operating states and parameters, it measures the likelihood of a particular combination of plant parameters actually occurring. For plant states which are very rare, some relaxation of the performance characteristics of the protective systems may be justified. This in turn helps to define both the allowed plant operating states and the safety limits.

When used in conjunction with 'best estimate' analysis, the uncertainty analysis can guide the code validation and the supporting R&D, concentrating them on the most likely, rather than on outlier, phenomena.

## II–4. TYPES OF UNCERTAINTY

There are three major sources of uncertainty in accident analysis [II–2, II–3]:

(a) *Code or model uncertainty*: Uncertainty associated with the models and correlations, the solution scheme, model options, unmodelled processes, data libraries and deficiencies of the computer programme.
(b) *Representation or simulation uncertainty*: Uncertainty in representing or idealizing the real plant, such as that due to the inability to model a complex geometry accurately, three dimensional effects, scaling, control and system simplifications.
(c) *Plant uncertainty*: Uncertainty in the measuring or monitoring of a real plant, such as reference plant parameters, instrument error, set points, instrument response.

There are other potential sources of uncertainty. The 'user effect', discussed elsewhere in this Safety Report (Section 7), can introduce a variability in computer code predictions. Sometimes the user effect is put in with the uncertainties just listed. However, the user effect can be mitigated by methods discussed in Section 7, such as proper code documentation, training, experienced supervision and cross-checking the results against similar calculations performed elsewhere. Similarly if the code does not converge spatially (number of nodes) or temporally (size of time steps), a variability can be introduced into the answers. These effects can also be mitigated, by performing a convergence study before a new accident analysis model is used. Even changes in the computer hardware or operating system software used to support the accident analysis code can result in changes in the predictions. Again, these changes can be minimized by proper testing procedures or by introducing new operating system software. While all these examples are potential traps for the unwary, they can all be minimized through effective quality assurance procedures for accident analysis. Therefore they are not covered further in this Annex. Analysis of each of the three sources of uncertainty — code, representation and plant — will now be discussed.

## II–5. UNCERTAINTY ANALYSIS TECHNIQUES

### II–5.1. Model uncertainties

Model uncertainties include uncertainties in comparison with the code of both separate effects and integral tests, as well as uncertainties in the experimental measurements themselves [II–4]. A code developer will normally derive these uncertainties in the code validation process; a user therefore needs to look into the code validation reports to determine what the model uncertainties are. This ideal cannot always be met: one may have to extrapolate from smaller scale experiments to the full scale plant. There may also be problems when test data specific to a particular reactor type simply do not exist.

It is important to focus the end point of the uncertainty analysis on parameters which are used directly in comparison with acceptance criteria, for example, the peak cladding temperature, the dose to the public and the peak containment pressure. Other parameters may not be used in acceptance criteria, for example, the extent of phase separation, or may be the result of an intermediate calculation and used only as input to the final calculation, for example, the xenon load. The latter situation will also occur when codes are linked, with intermediate results being passed from one code to another. One does not have to do an uncertainty analysis on each code making up the chain, but only on the chain itself. The purpose of uncertainty analysis is not to quantify the uncertainty in every prediction of every code that is used, but only in the parameters used directly in the comparison with acceptance criteria. The important quantities which contribute to these output parameters will have to be determined, together with their own uncertainties.

### II–5.2. Representation uncertainty

The amount of uncertainty introduced by the necessary simplifications in modelling a real plant can be estimated. These simplifications include geometrical simplifications, parameter ranges and local conditions. For example, it is not usually practical to model the thermohydraulics of all 380 fuel channels in a CANDU 6 — LOCA analysis typically uses between 5 and 20 coupled channels. However, a sensitivity study can be done for a representative LOCA analysis in which the number of channels in one core pass is increased from 5 to 10 to 20, and the change in the key safety parameters is noted. One then obtains a measure of the uncertainty in the results introduced by the geometrical simplification. Similarly, the change in hydraulic roughness of each pipe may not be known as the plant ages, but analysis using high and low bounding values can be performed to determine the sensitivity of the key results. Similar studies could be done for the radial and axial subdivision of the fuel channel in an LWR core, the modelling of the tube bundle in the steam

generators or the nodalization of the downcomer in the reactor pressure vessel of PWRs.

### II–5.3. Plant uncertainty

Plant uncertainty analysis uses the generally observable variation in plant parameters, plant states and set points as an input to the overall uncertainty analysis. Because there are thousands of plant parameters, one must first identify the sensitive ones (those which affect in a major way the accident analysis outputs used for comparison with the acceptance criteria). Observation of actual plant operation (or the use of historical plant records) can generate the actual statistical distribution of the sensitive parameters. If the method for uncertainty analysis is an overall statistical combination of uncertainties, these distributions can be incorporated.

Alternatively, one can define statistical 'points' for each operating parameter, such as 'operating centre', '90th percentile' and '99.9th percentile'. An acceptance criterion for accident analysis can be defined at each 'point' and compared with the results of the accident analysis. This approach allows less restrictive requirements, the further the operating parameter is from its normal state and the less often this occurs. The plant operation must then demonstrate in future that the statistical 'points' continue to be met.

## II–6. COMBINATION OF UNCERTAINTIES

Having identified the individual uncertainty components, one must then combine them to obtain an overall uncertainty in each parameter that is compared with an acceptance criterion. Given the large number of individual uncertainties and the complexity of the system analysis codes, this can rapidly become intractable unless some simplifying assumptions are made. Thus many approaches rely on expert judgement to reduce the amount of labour and computation time. Some of the approaches currently in use are now described.

One approach is based on the sensitivity to statistically based variations in *known* sensitive input parameters. The steps in applying this method are as follows:

(a) Identify and rank possible sources of modelling uncertainty;
(b) For those models ranked highly, determine the range of uncertainty;
(c) Perform sensitivity calculations for the accident using each of the highly ranked models;
(d) Derive a combined uncertainty by summing the individual uncertainties in quadrature.

If the number of input parameters is not too large, the system analysis codes can be used to generate sensitivities to these parameters, singly and in combination. Since in practice this can only be done for a small number of parameters, another approach is to derive simplified analytical representations of the functional dependence of the parameter, either through some knowledge of the underlying science, or simply as a Taylor series. The individual sensitivities are then combined using a driver code such as SUNSET [II–5] or SYVAC [II–6] to generate multidimensional response surfaces. These allow calculation of the uncertainty in the output safety parameter due to uncertainties in the input parameters used to generate the response surface.

## II–7. EXAMPLES OF APPLICATIONS OF UNCERTAINTY METHODS

A number of examples of applications of uncertainty methods are given. They are for illustrative purposes only and the results cannot be applied to cases other than those studied. Although there are a number of methods in use, they differ only in the relative weight given to the experimental, analytical and judgemental determination of uncertainties.

**Model uncertainties:** The OECD/CSNI has performed a study of various uncertainty methods. Five methods were compared in Ref. [II–7] for calculating the uncertainty in a 5% cold leg small break LOCA experiment in the large scale test facility at JAERI. The uncertainty method based on accuracy extrapolation (UMAE) extrapolates the accuracy of predictions from a set of integral experiments to the case being assessed. The other four methods rely on combinations of uncertainties in both models and data. The AEA Technology (AEAT) method defines reasonable ranges for uncertainties in phenomena and combines them. The GRS, IPSN and ENUSA methods assign subjective probability distributions to uncertainty ranges for uncertain input parameters and sample the resulting probability distribution to obtain a combined uncertainty. Table II–1 summarizes the features of the five models. Table II–2 shows the predicted uncertainty ranges using each method and the experimental value for the first and second peak cladding temperatures, the times at which these occur and the minimum core pressure drop.

**User effects:** This Safety Report has already indicated that user effects need not be treated in the same way as other uncertainties since they can be corrected or minimized. However, Fig. II–1 shows the effect of inadequate nodalization on the prediction for the mass inventory in CSNI International Standard Problem 18 [II–2].

**Combined uncertainty:** Figure II–2 [II–8] shows the uncertainty frequency distribution for the PCT during a PWR reflood, using the code scaling, applicability

TABLE II–1. SUMMARY OF METHODS COMPARED IN THE UNCERTAINTY METHODS STUDY

| Participant | Code version used | Method name and type |
|---|---|---|
| AEA Technology, UK | RELAP5/MOD3.2 | AEAT method: phenomena and uncertainties selected, quantified by ranges and combined. |
| University of Pisa, Italy | RELAP5/MOD2, cycle 36.04, IBM version, CATHARE 2, version 1.3U, rev. 5 | Uncertainty method based on accuracy extrapolation (UMAE). Accuracy in calculating similar integral tests is extrapolated to plant. |
| Gesellschaft für Anlagen- und Reaktorsicherheit (GRS), Germany | ATHLET, Mod 1.1, cycle A | GRS method: phenomena uncertainties quantified by ranges and subjective probability distributions (SPDs) and combined. |
| Institut de protection et de sûreté nucléaire (IPSN), France | CATHARE 2, version 1.3U, rev. 5 | IPSN method: phenomena uncertainties quantified by ranges and SPDs, and combined. |
| Empresa Nacional del Uranio, SA (ENUSA), Spain | RELAP5/MOD 3.2 | ENUSA method: phenomena uncertainties quantified by ranges and SPDs, and combined. |

and uncertainty evaluation method developed by the USNRC [II–9]. That paper combines code uncertainties derived from comparison with tests, plant parameter uncertainties and fuel parameter uncertainties.

## II–8. SUGGESTIONS

Uncertainty analysis goes hand in hand with the use of best estimate codes. The 'user' of system analysis codes can expect the developer to give an estimate of the model uncertainties. The user will need to generate the representation uncertainty through sensitivity studies on the plant being analysed. For operating stations, the user will need to generate plant uncertainty data from historical records.

TABLE II–2. UNCERTAINTY RANGES FOR POINT QUANTITIES

| Quantity | Limit | AEAT | Pisa RELAP5 | Pisa CATHARE | GRS | IPSN | ENUSA | Measured value |
|---|---|---|---|---|---|---|---|---|
| PCT1 | Upper | 938 | 773[a] | 693[a] | 904 | 813 | 1082 | 740 |
| (K) | Lower | 573 | 559[a] | 563[a] | 580 | 693 | 555 | — |
| PCT2 | Upper | 1142 | 620[a] | 681[a] | 849 | 653 | 1101 | 610 |
| (K) | Lower | 584 | 519[a] | 511[a] | 560 | 503 | 609 | — |
| $t_{PCT1}$ | Upper | 332 | 232 | 195 | 192 | 165 | 302 | 150 |
| (s) | Lower | 168 | 124 | 135 | 84 | 120 | 180 | — |
| $t_{PCT2}$ | Upper | 516 | 548 | 630 | 564 | 525 | 642 | 500 |
| (s) | Lower | 280 | 396 | 322 | 400 | 431 | 254 | — |
| $\Delta p_{min}$ | Upper | 5.55 | — | — | 15.3[b] | 15.3[b] | 3.41 | 3.8 |
| (kPa) | Lower | 0.63 | — | — | 2.2 | 0.75 | 0.44 | — |

[a] For Level 8 only; the other PCT values are maximized over all levels.

[b] Converted from collapsed liquid level.

The end point of the uncertainty analysis needs to quantify the uncertainties on those output parameters which are compared directly with the acceptance criteria for the accident. To do this the important quantities to which these output parameters are sensitive needs to be determined, together with their own uncertainties.

For countries with limited resources, either human or computational, it may not be practical to develop and combine a large number of uncertainties in a rigorous fashion. In that case one can use simplified techniques along the following lines:

(a) Determine the acceptance criteria for the accident.
(b) Determine those accident analysis output values which will be used to show compliance with the acceptance criteria.
(c) Employ experts and past experience to select and rank key accident analysis and plant data input parameters which are known to have an important effect on those output values.
(d) Perform sensitivity studies using the system analysis codes for variations in the key input parameters; if possible, determine the extent of variation from:
    (i) The known uncertainties in measurements of the physical parameters (e.g. the reactivity coefficient);
    (ii) The known uncertainties in plant parameters from actual plant records (e.g. the system flow and the trip set point variation);

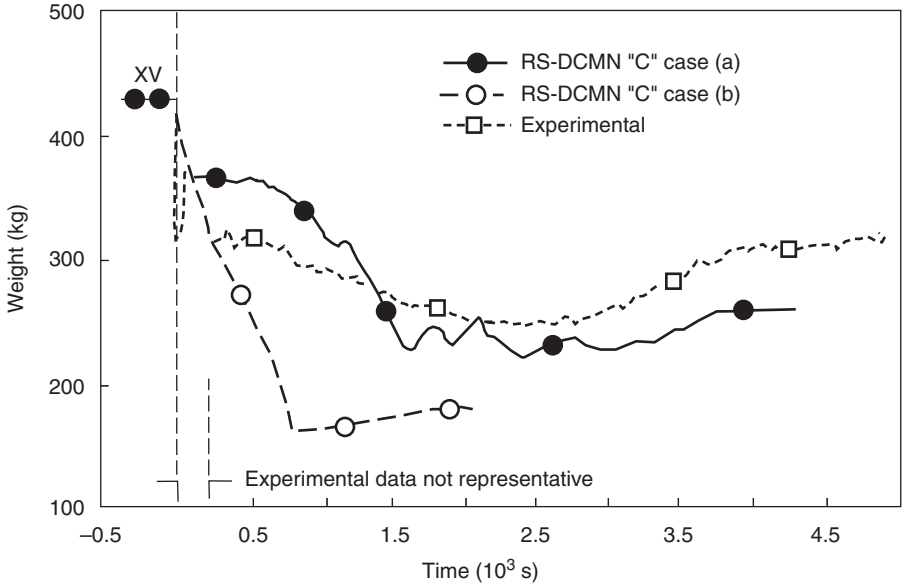



*Fig. II–1. Influence of a nodalization inadequacy on code results.*

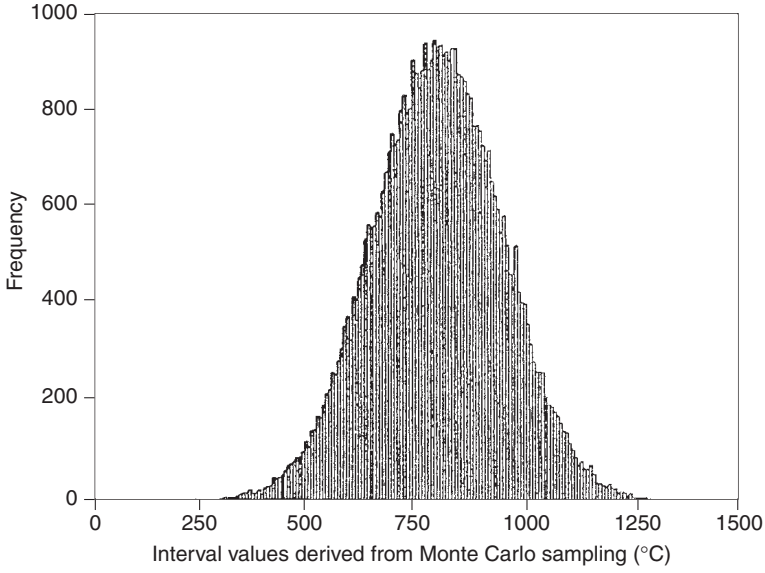



*FIG. II–2. Uncertainty frequency distribution for the PCT during a PWR reflood.*

(iii) The calculated or estimated uncertainties in the parameters using the behaviour of similar parameters elsewhere (e.g. the time constant of the amplifier in the protective system).

(e) Combine the input data uncertainties statistically to determine the prediction uncertainties in the output values used for comparisons with the acceptance criteria. Note that the key input parameters may not be independent in terms of variations in the output values. Expert judgement can usually anticipate dependences and suitable code cases chosen to evaluate them.

(f) Ensure that the code is spatially and temporally converged or optimized for the type of analysis used. In addition, ensure that the results do not vary from one computing platform to another. In this case, no representation uncertainty needs to be added. However, if the code is not spatially converged and it is impractical to run it with a sufficient number of nodes, perform a convergence study by increasing the number of nodes to determine how much change there is in the output parameters which are used for comparisons with acceptance criteria. Use this change as a measure of the uncertainty due to the plant representation.

(g) Determine the uncertainty due to the physical models in the code itself from the validation against experiment. This may not be rigorous owing to the lack of tests specific to the reactor characteristics, difficulties in scaling, etc.

(h) Combine the uncertainties from the above three steps (i)–(iii) to obtain an overall uncertainty in each of the output values used for comparisons with the acceptance criteria.

## REFERENCES TO ANNEX II


[II–1] NEWLAND, D.B., "The developing roles of best-estimate thermal-hydraulic calculations and uncertainty analyses in licensing in Canada", paper presented at OECD/CSNI Sem. on Best Estimate Methods in Thermal Hydraulic Safety Analysis, Ankara, 1998.

[II–2] D'AURIA, F., et al., "Overview of uncertainty issues and methodologies", paper presented at OECD/CSNI Sem. on Best Estimate Methods in Thermal Hydraulic Safety Analysis, Ankara, 1998.

[II–3] DUFFEY, R.B., et al., "Safety analysis: the treatment of uncertainty", paper presented at OECD/CSNI Sem. on Best Estimate Methods in Thermal Hydraulic Safety Analysis, Ankara, 1998.

[II–4] AMRI, A., "Use of best-estimate methods in a licensing case of 1300 MW(e) PWR", paper presented at OECD/CSNI Sem. on Best Estimate Methods in Thermal Hydraulic Safety Analysis, Ankara, 1998.

[II–5] REOCREUX, M., JANET, P., "Status of the French approaches for using best estimate codes in licensing", paper presented at OECD/CSNI Sem. on Best Estimate Methods in Thermal Hydraulic Safety Analysis, Ankara, 1998.

[II–6] ANDRES, T., SYVAC3 Parameter Distribution Package, Rep. AECL-10983, Atomic Energy of Canada Ltd, Montreal (1995).

[II–7] GLAESER, H., et al., "Application of uncertainty methods in the OECD/CSNI uncertainty methods study", paper presented at OECD/CSNI Sem. on Best Estimate Methods in Thermal Hydraulic Safety Analysis, Ankara, 1998.

[II–8] DEPISCH, F., et al., "Application of best estimate methods to LOCA in a PWR", paper presented at OECD/CSNI Seminar on Best Estimate Methods in Thermal Hydraulic Safety Analysis, Ankara, 1998.

[II–9] BOYACK, B.E., et al., An overview of the code scaling, applicability and uncertainty evaluation methodology, Nucl. Eng. Des. **119** (1990) 1–15.

## Annex III

## EXAMPLES ON THE DEVELOPMENT OF A SAFETY ANALYSIS DATABASE AND ENGINEERING HANDBOOK

In accordance with this Safety Report, two specific documents are used in the preparation of the input deck for computer codes:

(a) *Database for safety analysis*: This database contains all the information necessary to analyse the NPP, such as the geometry, thermohydraulic parameters, control system characteristics and set points, including drawings and other graphical documents. Since the requirements for the input data of modern codes for system transient analysis are similar, the database can be developed in code independent form.
(b) *Engineering handbook*: This document contains a full description of how the database has been converted into an input data deck for a specific computer code.

The pilot examples of the database [III–1] and the engineering handbook [III–2] have been elaborated in the framework of the IAEA Technical Co-operation Project RER/9/004 on Evaluation of Aspects for WWER-440 Model 213 Nuclear Power Plants, Reference Plant: Bohunice NPP V2 (Slovakia). The reference plant is equipped with a six loop WWER-440 reactor, with a thermal power of 1375 MW and has been operational since 1984. Here, updated examples of the aforementioned documents which have been elaborated recently for the same NPP are given.

The Database for Accident Analysis of Bohunice V2 NPP [III–3] is applicable to a broad spectrum of accidents ranging from 'best estimate' analysis of anticipated operational occurrences to analysis of BDBAs. Therefore, in addition to the usual descriptions of, for example, the primary and secondary systems, and the reactor protection system, attention was paid to giving an adequate description of the plant controllers and auxiliary systems as well as the containment (pressure suppression system and reactor cavity). However, some specific data for severe accident codes may be missing.

The aim was to develop a plant specific database. Therefore, the original data sources (such as drawings and technical documentation from the Bohunice V2 archive) were used where possible. Generic data were used only in a few specific cases (material properties, and characteristics of the main circulation pumps). In the development of the database there was close co-operation between the developers and the technical staff at Bohunice.

The database [III–3] is a large document of several hundred pages, with a significant portion devoted to figures, schematic layouts and tables. The contents list

of the document is provided in Section III–1. The database is split into ten relatively independent sections. However, details of the multilevel sections are given for only the first two sections of the document. Pagination is separate within each section. In order to minimize the duplication of data, there are some cross-links between sections. For example, the material properties of all important components, I&C and electricity supply of important systems and devices are summarized in separate sections; when the component or the plant system is being described in other sections, simple reference is made to these sections. The chosen form of the database enables independent checking, updating and upgrading of the data. The aim was to develop the database in an appropriate format for code users. Therefore, there are a number of axonometric figures describing the geometry of the piping systems. An example describing the pressurizer with its associated pipes is given (Figs III–1 to III–6).

Using the data from the database [III–3], a six loop input data deck (plant model) of a reference plant for the RELAP5/Mod3.2 code was developed. The aim was to develop an input data deck applicable to a broad spectrum of transients and accidents. Therefore, besides detailed nodalization of the primary and secondary systems, significant attention was also paid to the modelling of the core kinetics, ECCS, auxiliary systems, reactor protection system and plant controllers (startup and shutdown systems, pressurizer heaters, pressurizer spray, feedwater controller, reactor power controller, turbine controller, and steam dumps to the condenser and atmosphere). The final nodalization consists of about 900 control volumes, 1000 junctions, 800 heat structures and 3600 mesh points in heat structures. Furthermore, there are a number of control variables (≈700) and trips (≈600) used for describing the plant controllers. The nodalization scheme of the input data deck is shown in Figs III–7 to III–11.

As an intermediate step between the general database and the input data deck for the RELAP5/Mod3.2 computer code, an engineering handbook was prepared. An example of a description of pressurizer nodalization (hydrodynamic components and passive heat structures) is presented in Section III–2. The main reason for the preparation of the engineering handbook was to enable independent checking (as an essential part of quality assurance) of the input data and their correspondence with reference data given in the database.

The input data deck model was verified and validated using the systematic standard procedures given in Ref. [III–4] and the data for transients recorded in the WWER-440/V213 units operated (with on-transient level qualification). An example of input data deck validation using operational records is given in Figs III–12 to III–15 (where all six reactor coolant pumps are tripped [III–5]).

III–1. DATABASE FOR THE ACCIDENT ANALYSIS OF BOHUNICE V2 NPP

**List of contents**

1.2.2. Steam lines
1.2.3. Turbine
1.2.4. Generator
1.2.5. Condenser
1.2.6. Ejector of the condenser
1.2.7. Condensate pumps
1.2.7.1. Condensate pumps: first stage
1.2.7.2. Condensate pumps: second stage
1.2.8. Low pressure reheaters
1.2.8.1. Low pressure reheater No. 1
1.2.8.2. Low pressure reheater No. 2
1.2.8.3. Low pressure reheater No. 3
1.2.8.4. Low pressure reheater No. 4
1.2.8.5. Low pressure reheater No. 5
1.2.8.6. Subcooler of the low pressure reheater No. 1
1.2.8.7. Subcooler of the low pressure reheater No. 2
1.2.8.8. Subcooler of the low pressure reheater No. 4
1.2.8.9. Subcooler of the low pressure reheater No. 5
1.2.8.10. Condensate collector of the low pressure reheater No. 3
1.2.8.11. Condensate pump of the low pressure reheater No. 3
1.2.9. High pressure reheaters
1.2.9.1. High pressure reheater No. 1
1.2.9.2. High pressure reheater No. 2
1.2.10. Feedwater tank and deaerator
1.2.11. Condensate reheating system
1.2.12. Diameters of important pipes of the secondary system
1.2.13. Elevations
1.2.14. Feedwater pumps
1.2.15. Auxiliary feedwater pumps
1.2.16. Emergency feedwater pumps

1.3. HYDRAULIC CHARACTERISTICS OF PRIMARY SYSTEM

1.4. NEUTRON KINETICS

1.5. VALVES

1.6. REACTOR PROTECTION AND CONTROL SYSTEM

1.7. ELECTRICAL SYSTEMS

1.8. CONTAINMENT
1.9. CHARACTERISTICS OF MATERIAL
1.10. OPERATIONAL PARAMETERS AND REGIMES

APPENDIX 1. TECHNOLOGICAL SCHEMES
APPENDIX 2. TECHNICAL DRAWINGS

Only the sections relevant to this accident analysis report are listed below.

**Pressurizer**

The water volume of the pressurizer is connected via a T element and two parallel lines to the hot leg of the main circulation loop No. 1. The steam volume is connected via a pressurizer spray line to the cold leg of the same loop. All connections are on the non-isolable part of the main circulation loop.

*Pressurizer pressure vessel and internals:*

| | |
|---|---|
| • Internal diameter | 2.382 m [D39]* |
| • Internal heights: | |
| — Inner height of cylindrical part | 8.79 m [D39] |
| — Elliptical head at bottom | 2 × 0.701 m [D39] |
| — Total inner height of pressurizer | 10.192 m [D39] |
| • Wall thickness (including inner lining 9 mm thick): | |
| — Cylindrical part above pressurizer heaters | 0.154 m [D39] |
| — Cylindrical part on the level of pressurizer heaters | 0.199 m [D39] |
| — Elliptical head and bottom | 0.169 m [D39] |
| • Total internal volume | 44.0 $m^3$ [R28] |
| • Thickness of the insulation | 0.23 m [D43] |
| • Height of the spray above the pressurizer bottom | 9.392 m [D40, D39] |
| • Elevations of heaters above pressurizer bottom (on four levels separated from each other by 0.31 m) | 1.111–2.041 m [D39] |
| • Basic material of the pressurizer vessel | Steel 22K [R42] |
| • Mass of the pressurizer vessel (without coolant) · | 127 300 kg [R42] |
| • Total power of the pressurizer heaters | 1620 kW [R42] |
| • Power of one set of pressurizer heaters | 15 kW [R42] |
| • Number of sets of pressurizer heaters | 108 [R28] |
| • Powers of pressurizer heater groups are given in Section 6. | |

* References correspond to the list of references given in Ref. [III–3].

In terms of the electricity supply and control, the pressurizer heaters are arranged in five groups. The powers of individual groups of pressurizer heaters are given in Section 1.6.3.3 (Control of the Pressurizer Pressure). During nominal operation, only the first group of heaters is in operation.

The geometrical dimensions of the pressurizer surge lines and the location of the connecting point to the cold leg of loop 1 of the pressurizer vessel as well as the discharge lines to the bubbler tank are given in the following schemes.

## III–2. ENGINEERING HANDBOOK FOR THE RELAP5/MOD 3.2 INPUT DATA DECK OF THE BOHUNICE V2 NPP (AN EXAMPLE)

### III–2.1. **Pressurizer**

#### *III–2.1.1. Sources from the database*

All the data describing the pressurizer and its connections to the primary system (surge lines and spray pipework) are presented in the database in Sections 1.1.7.1 (Pressurizer). The pipework connecting the pressurizer with the bubbler tank is described in Section 1.1.7.2 (Bubbler Tank). All valves relevant to the pressurizer is described in Section 1.5.1.1 (Description of the Pressurizer Safety, Relief and Spray Valves). Control of the pressurizer level and pressure (pressurizer spray and heaters) is described in Sections 1.6.3.2 (Control of the Pressurizer Level) and 1.6.3.3 (Control of the Pressurizer Pressure), respectively. The material composition of the pressurizer walls is given in Section 1.9.1 (Presence of the Most Important Materials), and then the material properties are given in Section 1.9.4 (Steels). The nodalization of the pressurizer is shown on Fig. III–7.

#### *III–2.1.2. Hydrodynamic components*

The pressurizer vessel is a cylindrical structure with an elliptical bottom and head. In the nodalization scheme the volume of the pressurizer vessel is split into three hydrodynamic components:

*Component 706*: Elliptical bottom

— Type of element: Branch
— Total volume: $V = 2.72$ m$^3$
— Flow area: $A = 3.88$ m$^2$ (calculated by the code RELAP5/Mod3.2 from the expression $A = V/L$)

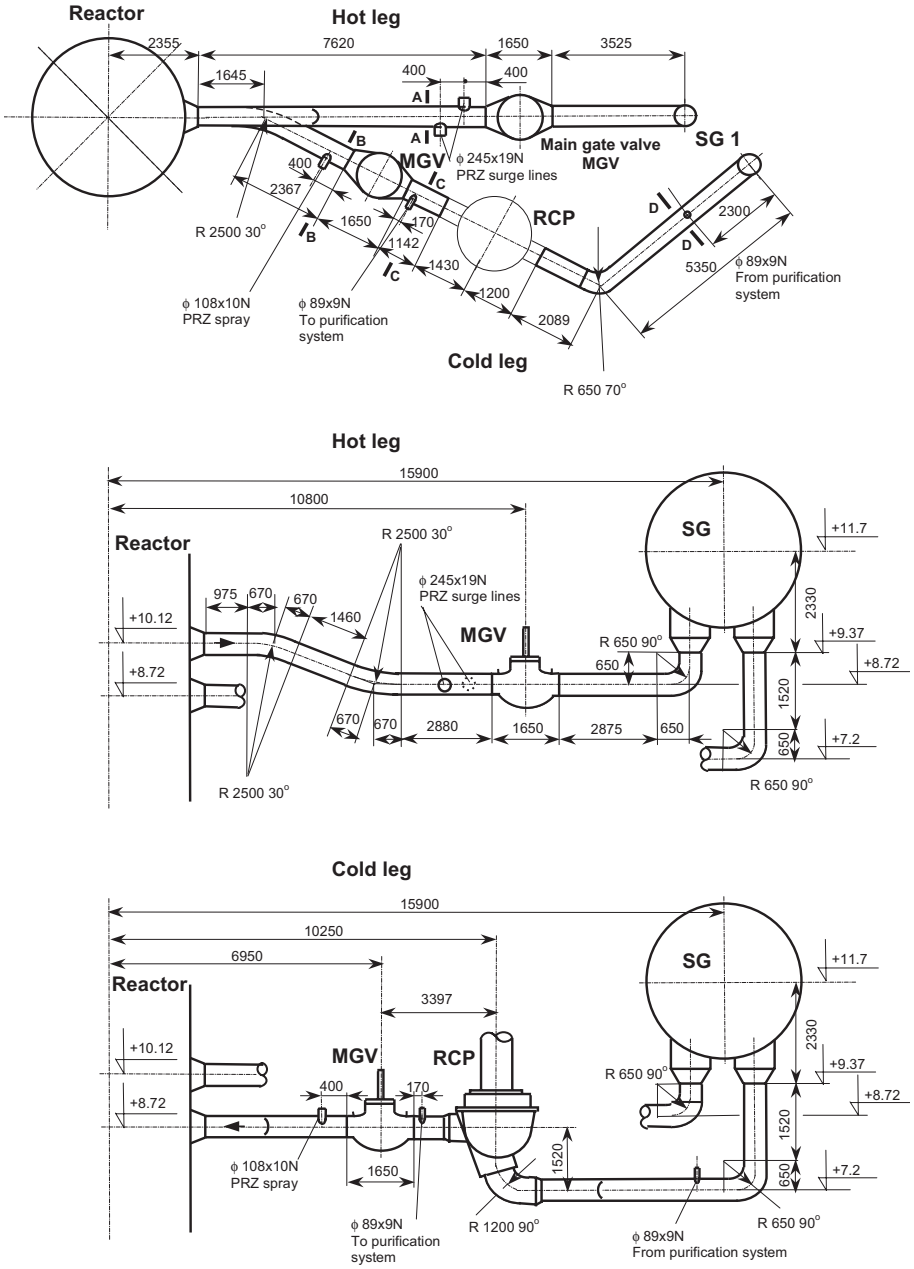



*FIG. III–1. Main circulation loop No. 1 (dimensions in millimetres).*

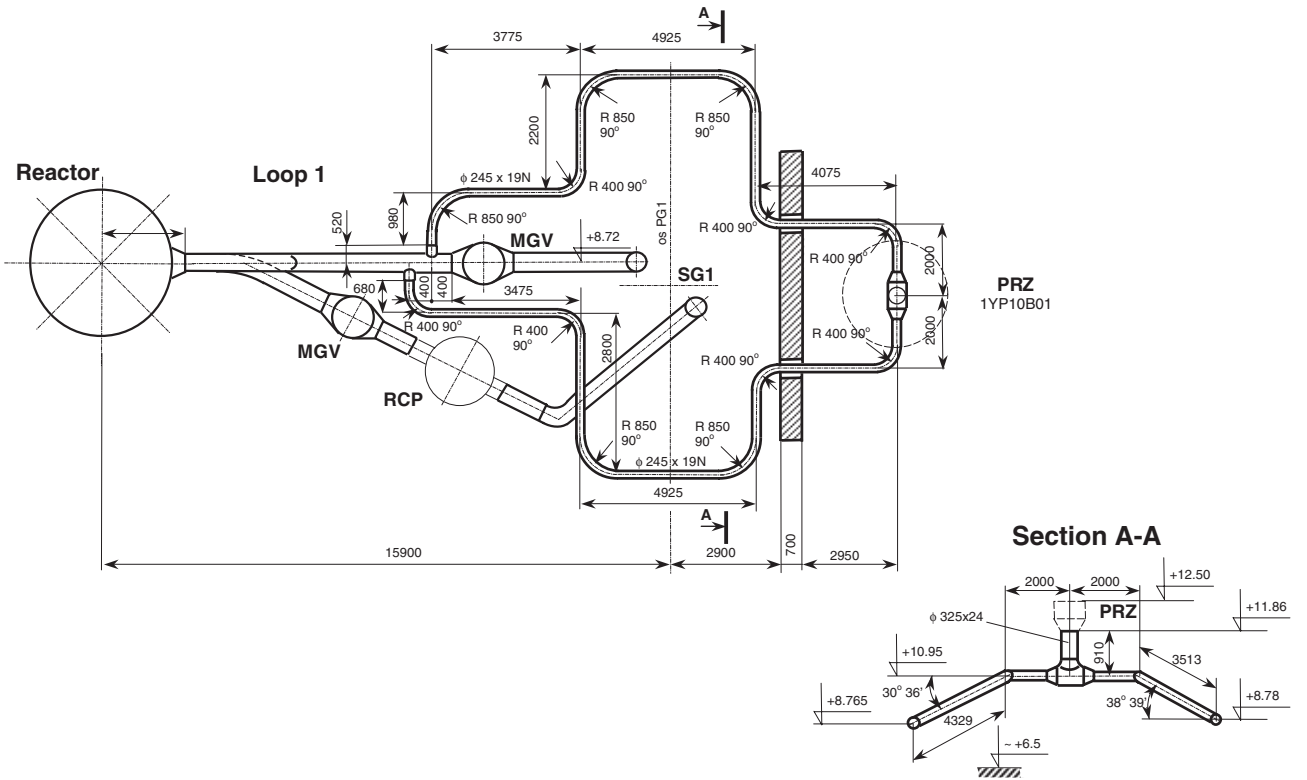
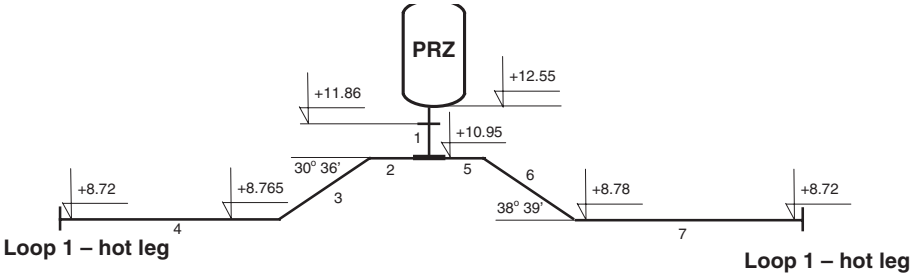



*FIG. III–2. Pressurizer surge lines (dimensions in millimetres).*




| Pressurizer surge lines | | | | | | | |
|---|---|---|---|---|---|---|---|
| Section number | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Length of section (mm) | 910 | 5731 | 4329 | 10613 | 5731 | 3513 | 11606 |
| Total length (mm) | 910 | 20673 (sections 2–4) | | | 20850 (sections 5–6) | | |
| Pipeline diameter (mm) | ø 325 × 24 | ø 245 × 19 | | | ø 245 ×19 | | |
| Pipe bends | | R 850 90° sections 3–4, 4 twice (total number: 3)<br>R 400 90° sections 2, 2–3, 4 (total number: 3) | | | R 850 90° sections 6–7, 7 (total number: 2)<br>R 400 90° sections 5, 5–6, 7 twice (total number: 4) | | |
| Pipeline label | | IYP10U07 | | | 1YP10U07 | | |

**Note**: In sections 2 and 5 a T tube (325 mm × 24 mm) is included (half the length in each section) as well as the transition from DN 300 to DN 200 (DN, diameter in millimetres).

*FIG. III–3. Simplified scheme of the pressurizer surge lines (dimensions in millimetres).*

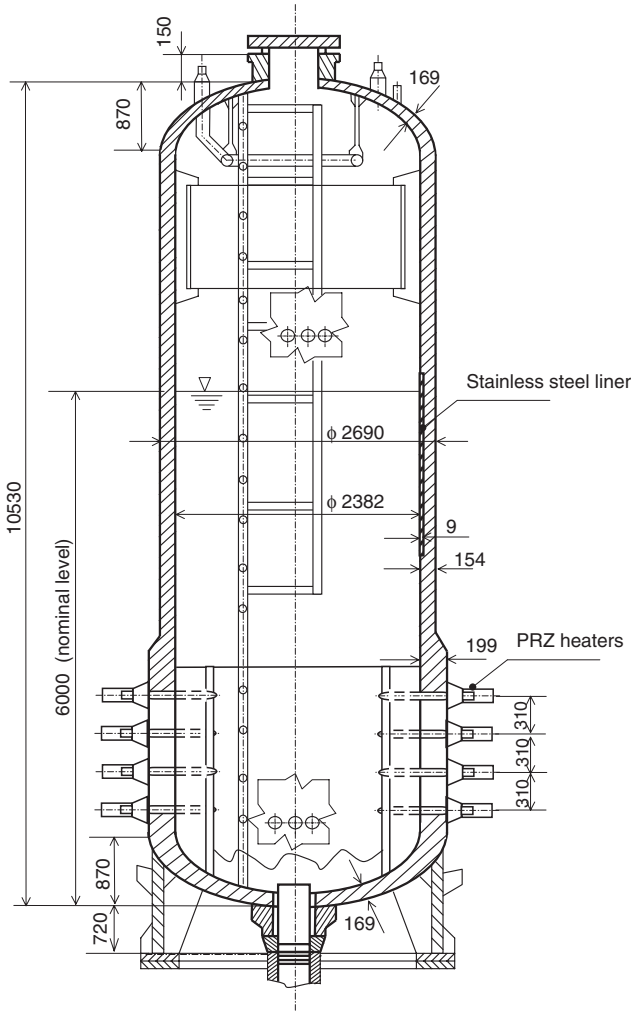
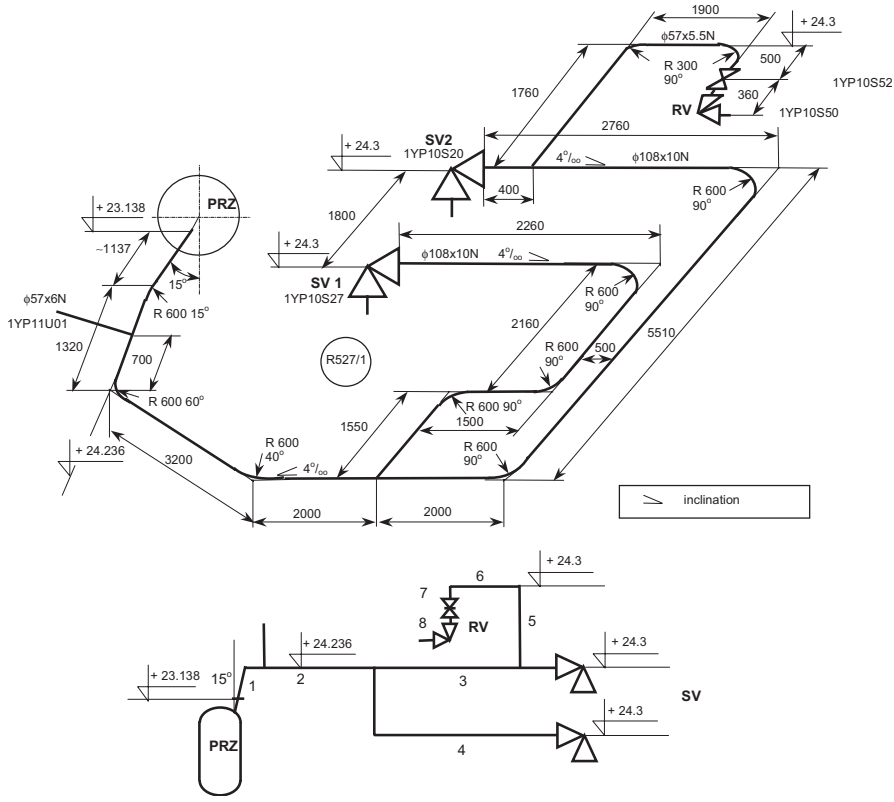
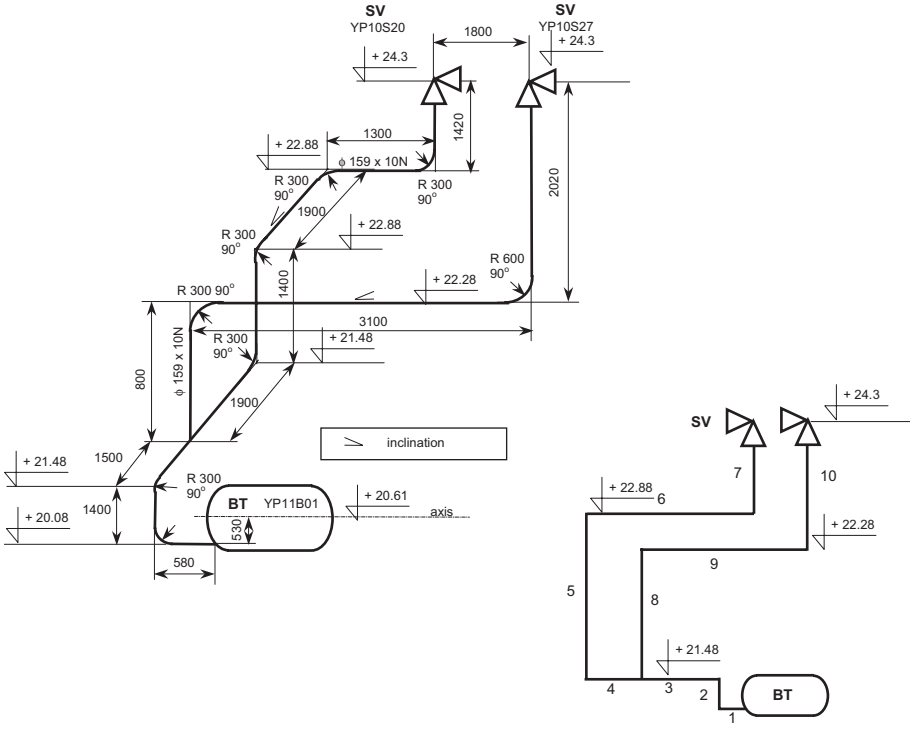



*FIG. III–4. The pressurizer (dimensions in millimetres).*




| Pipelines from pressurizer to safety valves and relief valves | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Section number | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Length of section (mm) | ≈1137 | 6428 | 9774 | 6696 | 1760 | 1642 | 500 | 360 |
| Total length (mm) | 24035 (sections 1–4) | | | | 4262 (sections 5–8) | | | |
| Pipeline diameter (mm) | ø 108 × 10N | | | | ø 57 × 5.5N | | | |
| Pipe bend | R 600 60° section 2 (total number 1)<br>R 600 90° sections 3 (twice)<br>and 4 (3 times)<br>(total number: 5)<br>R 600 15° between sections 1 and 2<br>(total number: 1)<br>R 600 40° section 2 (total number: 1) | | | | R 300 90°<br>between sections 5–6, 6–7<br>(total number: 2) | | | |
| Pipeline label | 1YP10U04 | | | | | | | |

*FIG. III–5. Pipelines from pressurizer to safety and relief valves (dimensions in millimetres).*




| Pipelines from safety valve to bubbler tank | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Section number | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Length of section (mm) | 451 | 1400 | 1371 | 1771 | 1400 | 2813 | 1420 | 800 | 2842 | 2020 |
| Total length (mm) | 10626 (sections 1–7) | | | | | | 5662 (sections 8–9) | | | |
| Pipeline diameter (mm) | ø 159 × 10N | | | | | | | | | |
| Pipe bend | R 600 90° between sections 9–10 (total number: 1)<br>R 300 90° between sections 1–2, 2–3, 4–5, 5–6, 6, 6–7, 8–9 (total number: 7) | | | | | | | | | |
| Pipeline label | 1YP11U02 | | | | | | | | | |

*FIG. III–6. Pipelines from safety valves to bubbler tank.*

— Length: $L = 0.701$ m
— Hydraulic diameter: $d_h = 2.222$ m (calculated by the code from the expression $A = \pi d_h^2/4$)
— Elevation: $H = 0.701$ m ($H = L$)

*Component 707*: Cylindrical part

— Type of element: Pipe
— Number of cells: 12
— Flow area: $A_1 = 4.0$ m$^2$ *; $A_2 = A_3 \cdots = A_{12} = 4.456$ m$^2$
— Lengths: $L_1 = 1.34$ m, $L_2 = L_3 = 0.85$ m, $L_4 = L_5 \cdots = L_{10} = 0.5$ m, $L_{11} = L_{12} = 1.125$ m
— Total pipe length: $L = S_{i=1-12}\, L_i = 8.79$ m
— Total volume: $V = 38.56$ m$^3$ (calculated by the code summing the volumes of all cells)
— Hydraulic diameter: $d_h = 2.257$ m for the first cell, $d_h = 2.382$ m for cells 2–12 (calculated by the code for each cell from the expression $A = \pi d_h^2/4$)
— Total elevation: $H = 8.79$ m ($H = L$).

*Component 708*: Elliptical head

— Type of element: Branch
— Total volume: $V = 2.72$ m$^3$
— Flow area: $A = 3.88$ m$^2$ (calculated by the code from the expression $A = V/L$)
— Length: $L = 0.701$ m
— Hydraulic diameter: $d_h = 2.222$ m (calculated by the code from the expression $A = \pi d_h^2/4$)
— Elevation: $H = 0.701$ m ($H = L$)

*III–2.1.3. Passive heat structures*

These structures represent the thick wall structure of the pressurizer vessel, which is made of carbon steel (22K) covered from the inner surface by a liner made of stainless steel (08Ch18N10T). In accordance with hydrodynamic component nodalization, the pressurizer walls are divided into four heat structures, representing:

* Comment: The flow area of the first cell is reduced due to the presence of pressurizer heaters.

— Elliptical bottom
— Elliptical head
— Lower (thicker) part of cylindrical structure (where the pressurizer heaters are located)
— Upper (thinner) part of cylindrical structure.

In total, seven computational points are used in the radial direction to model the temperature distribution and the heat flux through the wall. In the vicinity of the inner surface (stainless steel liner), the computational mesh is refined in order to represent properly large temperature gradients, which can be expected in accidents. On the outside surface, the thermal insulation is not modelled. Instead, a convective boundary condition is used and the heat transient coefficient is tuned in order to obtain the correct heat losses from the pressurizer for a given temperature in the corresponding compartment (the steam generator boxes).

*Heat structure 173*: Elliptical bottom

— Geometry type: Rectangular
— Surface area: 6.07 $m^2$
— Composition: Tables 604 and 652 (tables describing thermal property data)
— Number of radial points: 7
— Mesh: See input data deck
— Left boundary: Convective; component 706
— Right boundary: Convective; heat transfer coefficient prescribed by Table 939, temperature in confinement (SG boxes) prescribed by Table 942.

*Heat structure 172*: Lower (thicker) part of cylindrical structure

— Geometry type: Cylindrical
— Inner diameter: 1.191 m
— Outer diameter: 1.39 m
— Surface area: Calculated for each axial node by the code from a given radius
— Composition: Tables 604 and 652 (tables describing thermal property data)
— Number of axial points: 2
— Number of radial points: 7
— Mesh: See input data deck

— Left boundary: Convective; component 707, cells 707-1 and 707-2
— Right boundary: Convective; heat transfer coefficient prescribed by Table 939, temperature in confinement (SG boxes) prescribed by Table 942.

*Heat structure 173*: Upper (thinner) part of cylindrical structure

— Geometry type: Cylindrical
— Inner diameter: 1.191 m
— Outer diameter: 1.345 m
— Surface area: Calculated for each axial node by the code from a given radius
— Composition: Tables 604 and 652 (tables describing thermal property data)
— Number of axial points: 10
— Number of radial points: 7
— Mesh: See input data deck
— Left boundary: Convective; component 707, cells 707-3–707-12
— Right boundary: Convective; heat transfer coefficient prescribed by Table 939, temperature in confinement (SG boxes) prescribed by Table 942.

*Heat structure 174*: Elliptical head

— Geometry type: Rectangular
— Surface area: 6.07 $m^2$
— Composition: Tables 604 and 652 (tables describing thermal property data)
— Number of radial points: 7
— Mesh: See input data deck
— Left boundary: Convective; component 708
— Right boundary: Convective; heat transfer coefficient prescribed by Table 939.

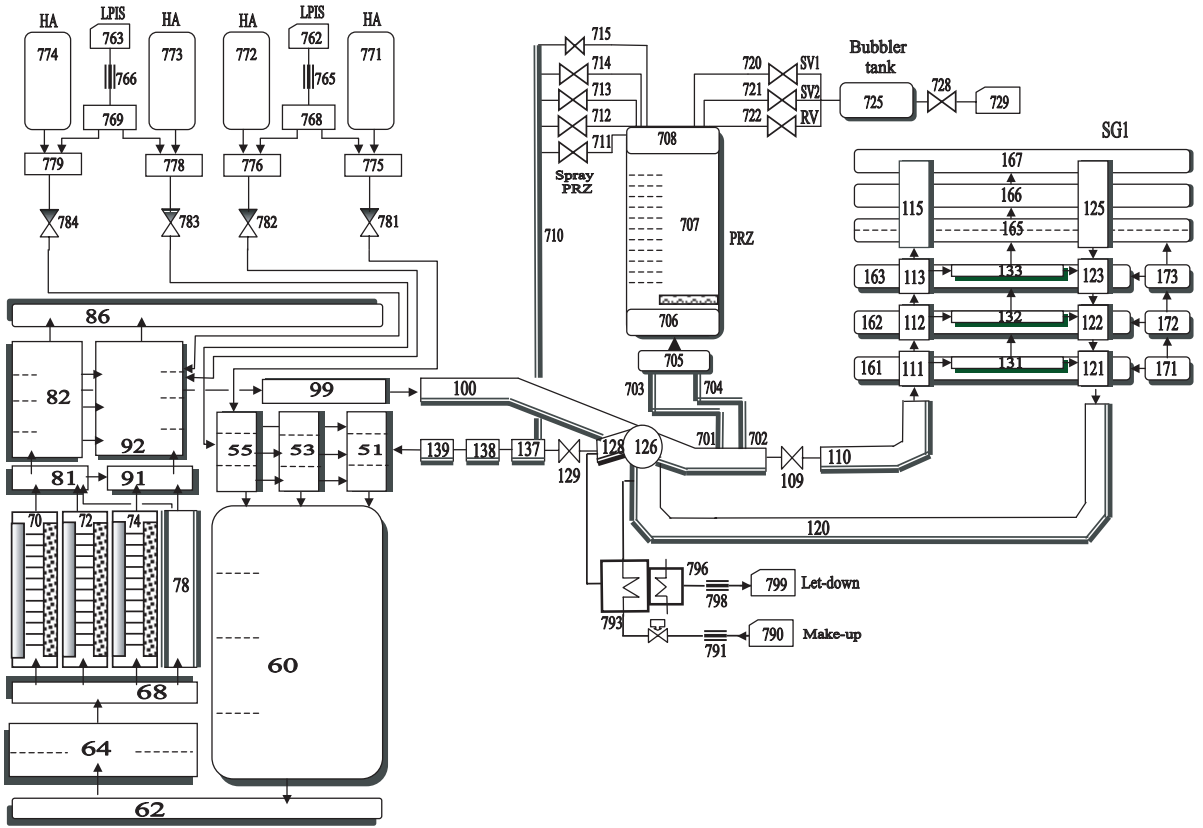



*FIG. III–7. Nodalization scheme of the reactor vessel and loop 1.*

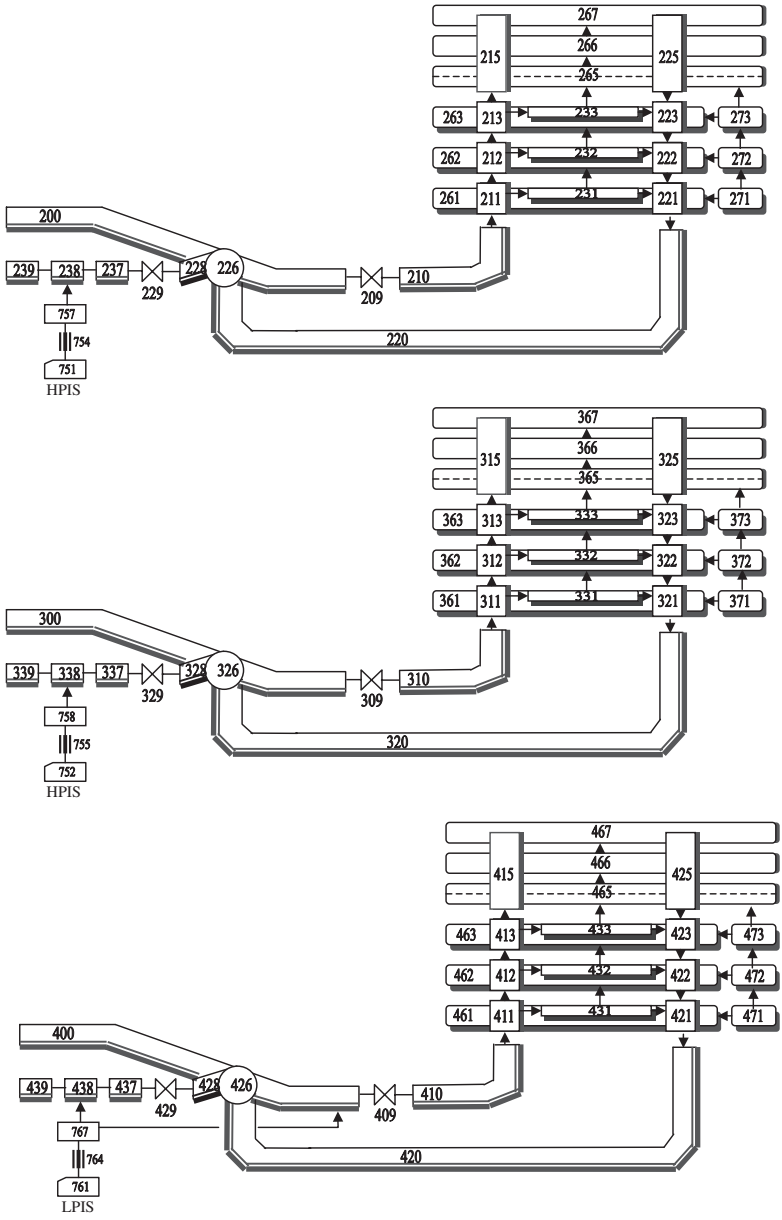



*FIG. III–8. Nodalization scheme of loops 2, 3 and 4.*

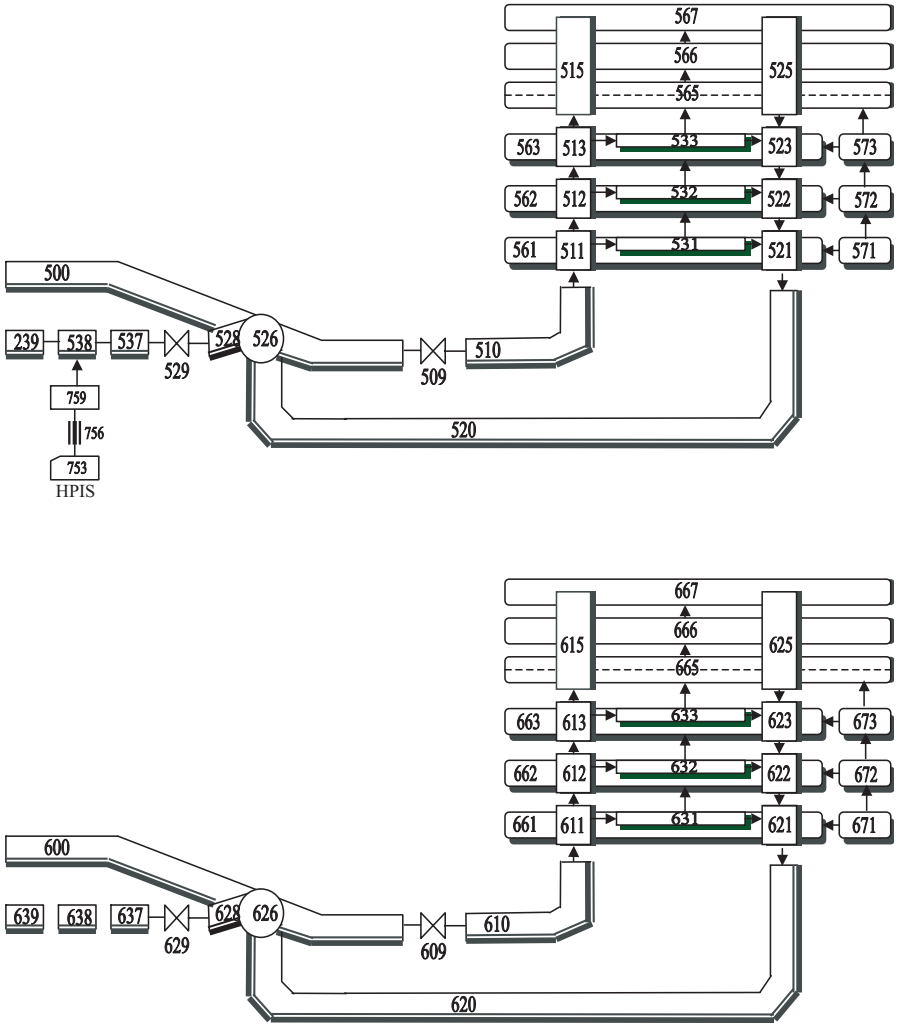



*FIG. III–9. Nodalization scheme of loops 5 and 6.*

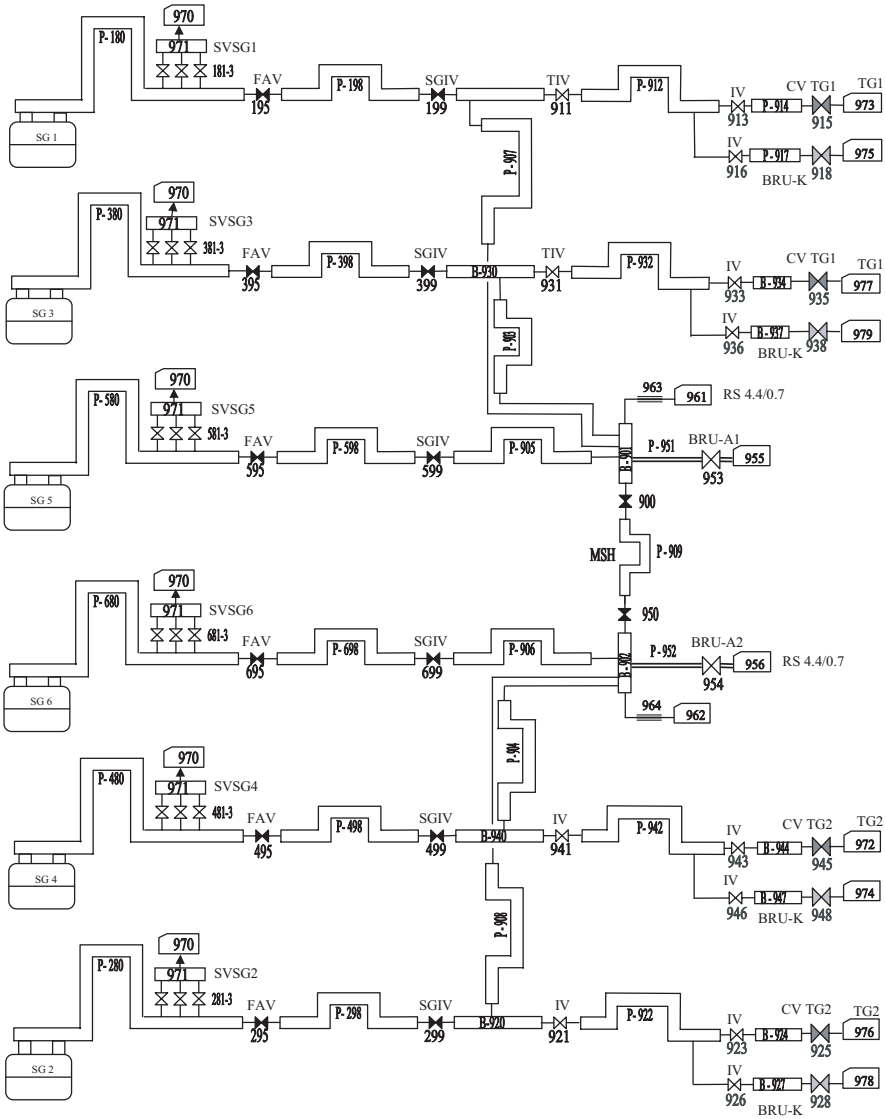



*FIG. III–10. Nodalization scheme of the secondary steam system.*

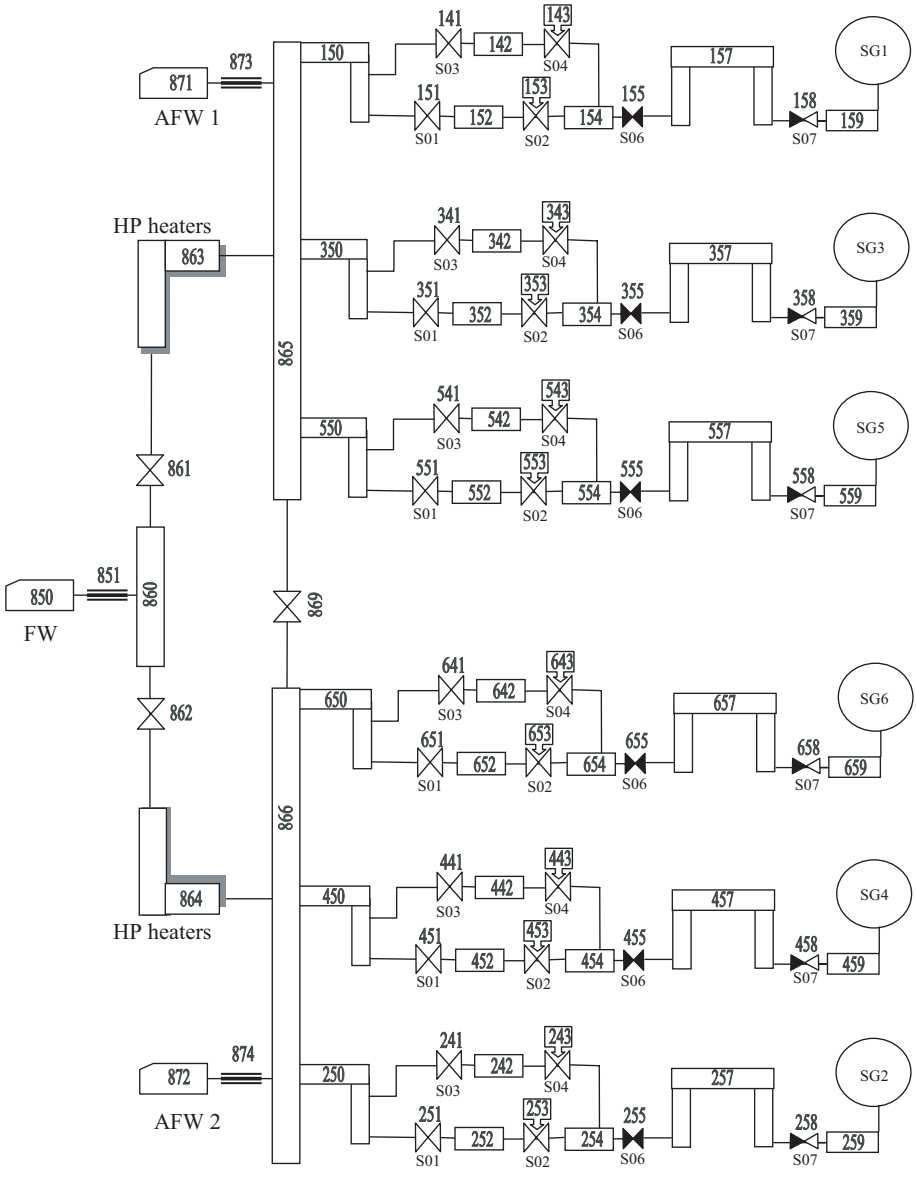



*FIG. III–11. Nodalization scheme of the feedwater system.*

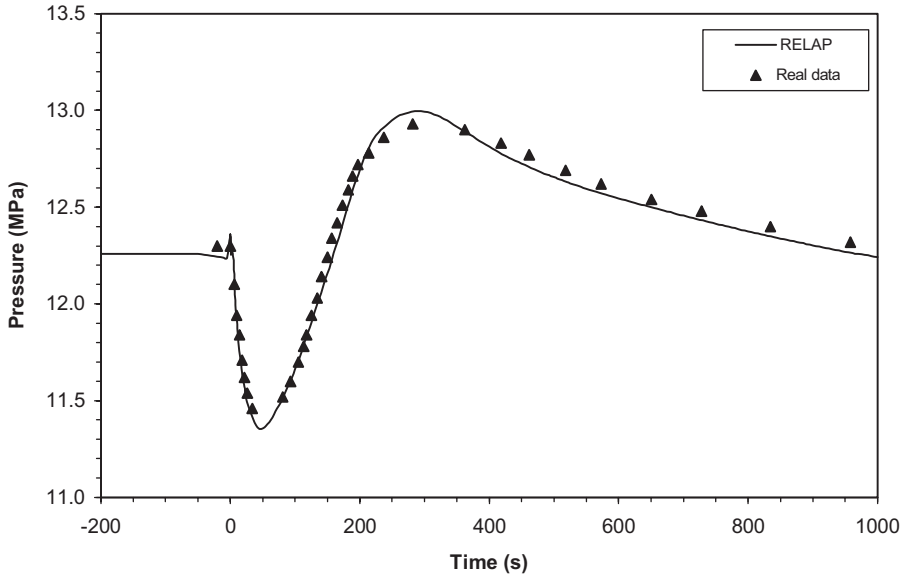



*FIG. III–12. Primary pressure. Input data deck validation when all RCPs are tripped. Comparison of prediction made using the RELAP/Mod3.2 code with real data.*

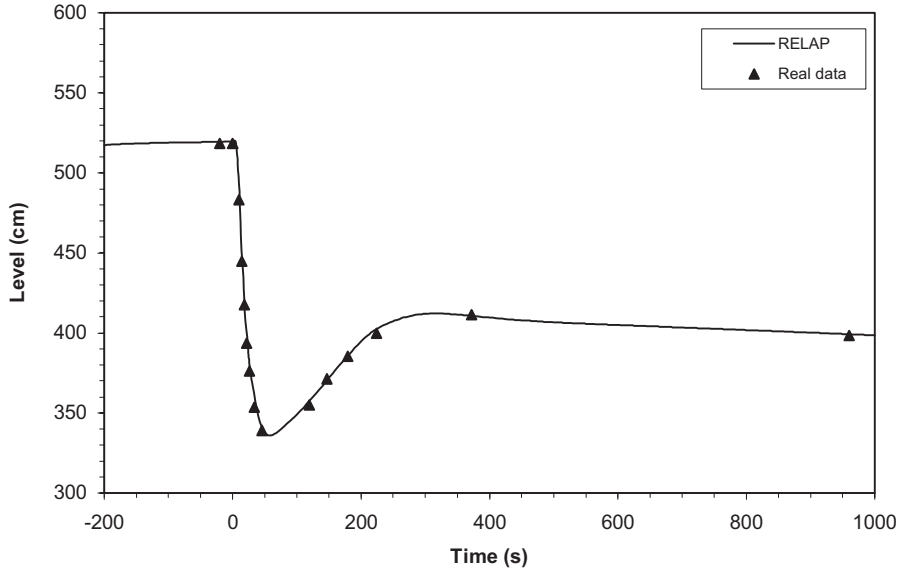



*FIG. III–13. Collapsed water level in pressurizer. As for Fig. III–12.*

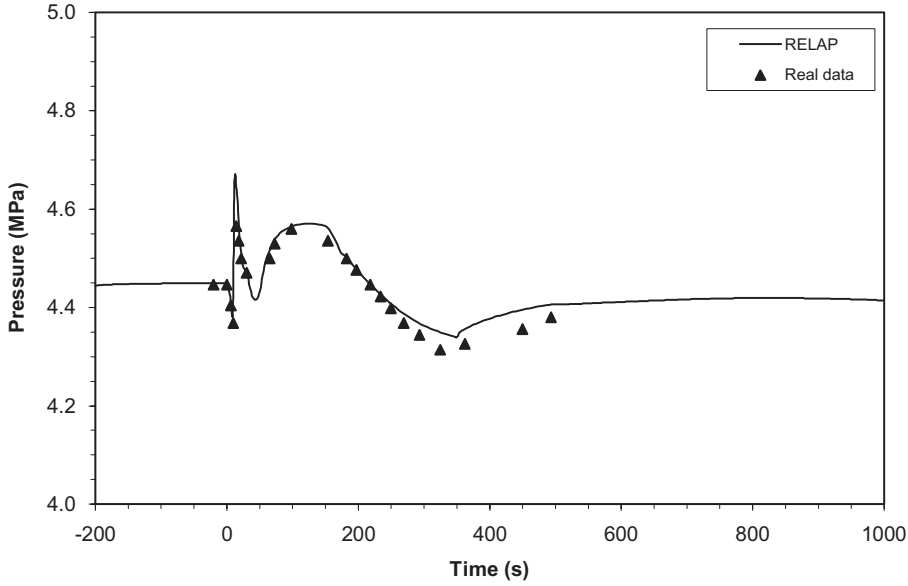



*FIG. III–14. Pressure in main steam header. As for Fig. III–12.*

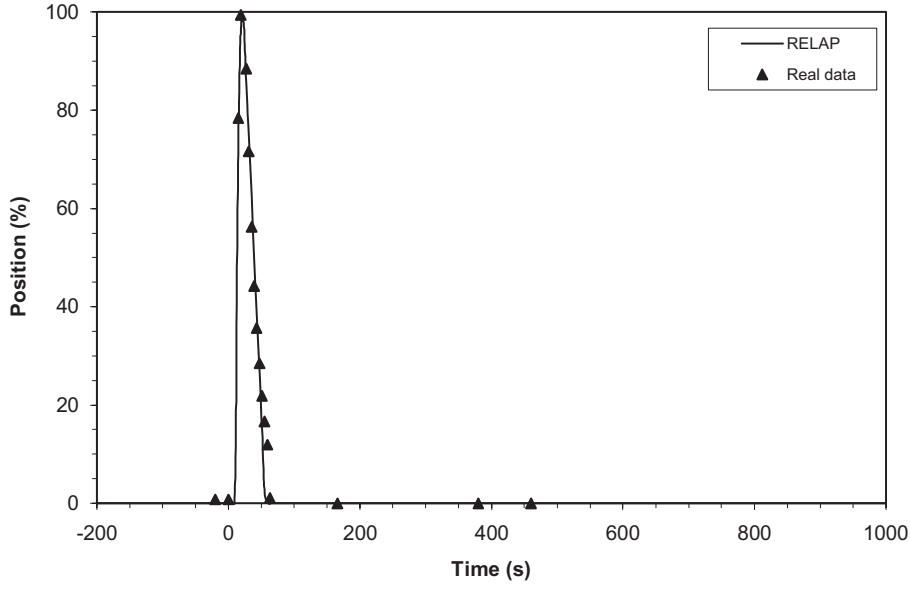



*FIG. III–15. Position of left steam dump to condenser, TG No. 2. As for Fig. III–12.*

## REFERENCES TO ANNEX III


[III–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Database for the Safety Analysis of WWER-440 Model 213 Nuclear Power Plants, Rep. TC/RER/004-A041, IAEA, Vienna (1994).

[III–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Handbook for the Safety Analysis of WWER-440 Model 213 Nuclear Power Plants, Rep. TC/RER/004-A042, IAEA, Vienna (1994).

[III–3] INZINICRSKA VYPOCTOVA SPOLOCNOST TRNAVA, Database for the Accident Analysis of Bohnice V2 NPP, Revision 0, IVS, Bratislava (1999) (elaborated by IVS Trnava).

[III–4] D'AURIA, F., et al., "A methodology for the qualification of thermal-hydraulic code nodalizations", paper presented at 6th Int. Top. Mtg on Nuclear Reactor Thermal Hydraulics, Grenoble, 1993.

[III–5] MATEJOVIC, P., VRANKA, L., BACHRATY, M., "Validation of RELAP5/Mod3.2 using data recorded at operated VVER-440 units", paper presented at ASME&JSME Joint Fluid Engineering Conf. San Francisco, 1999.

## Annex IV

## EXAMPLES OF COMPUTER CODES

The examples included in this Annex are not intended to represent an exhaustive listing of all possible codes which are used to support the analysis of nuclear plants. In many cases, the examples may become outdated as codes are merged or replaced by more capable codes. The inclusion of any code is not intended as an endorsement of that code or to indicate the applicability of that code for the indicated category. For many of the codes listed, additional and more complete references may be easily obtained. Users interested in more detailed information on these codes are encouraged to search for current references or to contact the organizations concerned. Where possible, the examples also include the country of origin of the code or, in some cases, the countries where special versions of those codes have been developed. In those examples that are given as international as the country of origin, the codes, or special versions of codes developed in a single country, are being developed through international consortia consisting of organizations based in more than one country. Many of the code examples, particularly the system thermohydraulic codes, are widely used in a number of countries. No attempt has been made to list the countries where these codes are used. However, current references may provide some indication of the countries where the codes are in extensive use.

For anticipated transients and DBAs, the examples are organized into the following six categories:

(a) Reactor physics codes;
(b) Fuel behaviour codes;
(c) Thermohydraulic codes including system, subchannel and CFD codes;
(d) Containment analysis codes, possibly also with radioactive transport features;
(e) Atmospheric dispersion and dose codes;
(f) Structural analysis codes.

Many of these codes are used in combination and may, on the basis of recent development activities, be merged to form more comprehensive code packages. In particular, reactor physics, subchannel or CFD codes may be incorporated into system thermohydraulic codes. Many of the system thermohydraulic codes have also been extended through the addition of severe accident models so that they can treat a wide range of accident conditions, including transients and design basis, beyond design basis and severe accident transients. In most cases, the extended codes will be obvious.

The reactor physics codes are used for a variety of applications including spectral analysis, preparing group libraries for dynamic codes and performing dynamic analyses of reactor cores. In some cases, the codes include spatial effects, one dimensional and three dimensional, and may include simplified thermohydraulic models. Some of the codes, or models in these codes, are increasingly being used together with system thermohydraulic codes to perform coupled core kinetics and system analysis for transient and DBA conditions. Examples include WIMS [IV–1], DYN3D [IV–2], KIKO 3D [IV–3] (Hungary), HEXTRAN [IV–4] (Finland) and COCCINELLE [IV–5] (France).

The fuel behaviour codes describe the behaviour of individual fuel rods in normal operating and DBA conditions. Examples of codes in this category include FRAPCON [IV–6] and FRAPT-T6 [IV–7] (USA), TRANSURANUS [IV–8] (Germany), ENIGMA [IV–9] (United Kingdom), START-3 [IV–10] and RAPTA-5 [IV–11] (Russian Federation), and ELESIM [IV–12] and ELOCA [IV–13] (Canada).

System thermohydraulic codes describe the behaviour of the reactor systems, including hydrodynamics, heat transfer, reactor kinetics, control systems and other system components. Examples of codes in this category include RELAP5 [IV–14], TRAC-P/B (PWR/BWR) [IV–15, IV–16] and COBRA-TRAC [IV–17] (USA), CATHARE [IV–18] (France), ATHLET [IV–19] (Germany), DINAMIKA [IV–20] (Russian Federation), SMABRE [IV–21] and APROS [IV–22] (Finland), and CATHENA [IV–23] and TUF [IV–24] (Canada).

The containment codes describe the thermohydraulics associated with the containment systems and components, including in some cases, hydrogen combustion. Examples include CONTEMPT [IV–25] and CONTAIN [IV–26] (USA), GOTHIC [IV–27] (Germany), JERICHO [IV–28], RALOC [IV–29] and COCOSYS [IV–30].

The structural analysis codes describe the behaviour of the vessel, piping and containment under various accident conditions. Although a large number of commercially available codes can be used, the codes used for reactor safety analysis applications include NASTRAN [IV–31], ABAQUS [IV–32], ANSYS [IV–33], SAP200 [IV–34] and COSMOS/M [IV–35].

The mechanistic system thermohydraulic codes which can be used for severe accident analysis as well as design basis analysis include SCDAP/RELAP5 [IV–36] (USA), CATHARE/ICARE [IV–35] (France), ATHLET-CD [IV–37] (Germany) and RELAP/SCDAPSIM [IV–38] (international). As the names imply, these codes are extended versions of RELAP, CATHARE and ATHLET noted in a preceding paragraph. IMPACT [IV–39] (Japan) is an advanced severe accident code being developed as a plant simulator. IMPACT currently uses RELAP for the thermohydraulic portion of the code.

The parametric codes include ESCADRE [IV–40] (France), ESTER [IV–41] (European Community), MAAP [IV–42], MELCOR [IV–43] (USA) and THALES [IV–44] (Japan).

## REFERENCES TO ANNEX IV


[IV–1] DONELLY, J.V., WIMS-CRNL: A User's Manual for the Chalk River Version of WIMS, Rep. AECL-8955, Atomic Energy of Canada Ltd, Chalk River (1986).

[IV–2] GRUNDMANN, U., ROHDE, U., DYN3D/M2: A Code for Calculation of Reactivity Transients in Cores with Hexagonal Geometry, Rep. FZR 93-01, Research Centre Rottendorf (1993).

[IV–3] KERESZTURI, A., "KIKO 3D: A three dimensional kinetics code for VVER-440", paper presented at the ANS Winter Mtg, Washington, DC, 1994.

[IV–4] KYRKI-RAJAMAEKI, R., RAETY, H., "Coupled Neutronics and Thermal-Hydraulic Modelling in Reactor Dynamics Codes TRAB-3D and HEXTRAN", paper presented at the 2nd CSNI Specialist Mtg on Simulators and Plant Analysers, Espoo, 1997.

[IV–5] GONZALEZ, R.F., FICHOT, F., CHATELARD, P., "Status of ICARE2 and ICARE/CATHARE Development", paper presented at the Winter ANS Mtg, Washington, DC, 1996.

[IV–6] BERNA, G.A., et al., FRAPCON-2: A Computer Code for the Calculation of Steady State Thermal-Mechanical Behaviour of Oxide Fuel Rods, Rep. NUREG/CR-1845, US Govt Printing Office, Washington, DC (1981).

[IV–7] SIEFKEN, L.J., et al., FRAPT-T6: A Computer Code for the Transient Analysis of Oxide Fuel Rods, Rep. NUREG/CR-2148, EGG-2104, US Govt Printing Office, Washington, DC (1981).

[IV–8] LASSMANN, K., TRANSURANUS: A fuel rod analysis code ready for use, J. Nucl. Mater. **188** (1988) 295–302.

[IV–9] KILGOUR, W.J., The ENIGMA Fuel Performance Code, User's Guide, Nuclear Electric, Berkeley Nuclear Laboratories, CA (1992).

[IV–10] MEDVEDEV, A.V., et al., Verification of the START-3 Program used for Strength and Thermophysical Calculations of a Full Scale Fuel Element under Base Load and Load Follow Operation in Power Reactors, Rep. SRC VNI/AEM, Moscow (1997).

[IV–11] BIBILASHVILI, Y.K., et al., "RAPTA-5 Code: modelling behaviour of VVER-type fuel rods in design basis accidents verification and calculations", Behaviour of LWR Core Materials under Accident Conditions, IAEA-TECDOC-921, IAEA, Vienna (1996) 139.

[IV–12] BUNGE, J.M., IGLESIAS, F.C., ELESIM-ii (Mod. 10), Rep. AECL-CRNL-2011-1, Atomic Energy of Canada Ltd, Chalk River (1982).

[IV–13] WALSWORTH, J.A., SILLS, H.S., High Temperature Transient Fuel Performance modelling: ELOCA, ME 4, Rep. AECL-CRNL-2010-1, Atomic Energy of Canada Ltd, Chalk River (1984).

[IV–14] FLETCHER, C.D., SCHULTZ, R.R., RELAP5/MOD3 Code Manual, Vol. 2, Rep. NUREG/CR 5535, INEL-95/0174, US Govt Printing Office, Washington, DC (1995).

[IV–15] LILES, D.R., et al., TRAC-PF1/MOD1: An Advanced Best-Estimate Computer Program for PWR Thermal-Hydraulic Analysis, Rep. NUREG/CR-4442, US Govt Printing Office, Washington, DC (1986).

[IV–16] BOSKOWSKI, J.A., et al., TRAC-BF1/MOD1: An Advanced Best-Estimate Computer Program for BWR Accident Analysis, Rep. NUREG/CR-4356, EGG-2625, US Govt Printing Office, Washington, DC (1992).
[IV–17] THURGOOD, M.J., et al., COBRA/TRAC: A Thermal–Hydraulics Code for Transient Analysis of Nuclear Reactor Vessels and Primary Coolant Systems, NUREG/CR-3046, US Govt Printing Office, Washington, DC (1983).
[IV–18] FASRVACQUE, M., Users' Manual of CATHARE 2 V1.3 E, Rep. STR/LML/EM/91-61, Grenoble (1992).
[IV–19] LERCHL, G., AUSTREGESILO, H., ATHLET MOD 1.1, Cycle C, Users' Manual, Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Garching (1995).
[IV–20] Computer Code: Calculation of Transient Regimes of Power Plants with VVER Reactors: DINAMIKA 5M, Technical Specifications No. 8624606.00311-019101-LU, GKAE-OKB, Gidropress, Moscow (1987) (in Russian).
[IV–21] MIETTINEN, J., "Development and assessment of the SBLOCA code SMABRE", paper presented at Mtg on Small Break LOCA Analysis in LWRs, Pisa, 1985.
[IV–22] PUSKA, E.K., MIETTINEN, J., HAENNINEN, M., KONTIO, H., KONKOILA, H., "APROS simulation system for nuclear power plant analysis", paper presented at 3rd JSME/ASME Joint Int. Conf. on Nuclear Engineering, Phoenix, 1995.
[IV–23] HANNA, B.N., CATHENA: A thermohydraulic code for CANDU analysis, Nucl. Eng Des. **180** (1997) 113.
[IV–24] LUXAT, J.C., et al., "Methodology, status and plans for development and assessment of TUF and CATHENA codes", in Transient Thermal-Hydraulics and Neutronic Code Requirements (Proc. OECD/CSNI Workshop Annapolis, 1996), Rep. NUREG/CP-0159, NEA/CSNI/R, U.S. Nuclear Regulatory Commission, Rockville, MD (1997) 4.
[IV–25] US NUCLEAR REGULATORY COMMISSION, CONTEMPT 4/ MOD 5: An Improvement to CONTEMPT 4/ MOD 4 Multicompartment Containment System Analysis Program for Ice Containment Analysis, Rep. NUREG/CR-4001, BNL, US Govt Printing Office, Washington, DC (1984).
[IV–26] MURATA, K.K., et al., Users' Manual for CONTAIN 1.1: A Computer Code for Severe Nuclear Reactor Accident Containment Analysis, Rep. NUREG/CR-5020, SAND 87-2309R4, Sandia National Laboratories, Albuquerque, NM (1989).
[IV–27] FISCHER, K., et al., "Batelle-Europe verifications and extensions of the GOTHIC code", paper presented at 5th Int. Top. Mtg on Reactor Thermal Hydraulics, Salt Lake City, 1992.
[IV–28] COMMANDE, A., TARABELLI, D., The ESCADRE Code System (Version Mod 1.0), JERICHO Users Manual, Rep. NT SEMAR 95/51, Paris (1995).
[IV–29] GESELLSCHAFT FÜR REAKTORSICHERHEIT, RALOC MOD 4.0 Cycle AD, Program Reference Manual, Gesellschaft für Reaktorsicherheit mbH, Garching (1996).
[IV–30] WEBER, G., SCHWARZ, S., "Analysis of the multi-compartment containment aerosol behaviour with COCOSYS", paper presented at OECD/CSNI Workshop, Cologne, 1998.
[IV–31] MSC.SOFTWARE CORP., MSC.NASTRAN, Version 70.7, User Manual, Los Angeles, CA (2000).

[IV–32] HIBBITT, KARLSSON&SORENSEN INC., HKS/ABAQUAS Version 5.8, User Manual, HKS, Pawtucket, RI (1999).
[IV–33] ANSYS INC., ANSYS, Version 5.6, User Manual, Canonsburg, PA (1999).
[IV–34] CSI INC., CSI/SAP200, User Manual, Berkeley, CA (1999).
[IV–35] STRUCTURAL RESEARCH AND ANALYSIS CORP., SRAC/COSMOS/M, User Manual, Los Angeles, CA (1999).
[IV–36] ALLISON, C.M., et al., in SCDAP/RELAP5/MOD3.1 Code Manual (Vols 1–5), Rep. NUREG/CR-6150, EGG-2720, US Govt Printing Office, Washington, DC (1993).
[IV–37] TRAMBAUER, K., "The code ATHLET-CD for the simulation of severe accidents in light water reactors", paper presented at 5th Int. Top. Mtg on Nuclear Reactor Thermal Hydraulics, Salt Lake City, 1992.
[IV–38] ALLISON, C.M., HAGMAN, D.L., "SCDAPSIM reactor system analyzer for design and beyond design basic accident conditions", paper presented at 5th Int. Conf. on Simulation Methods in Nuclear Engineering, Montreal, 1996.
[IV–39] UJITA, H., et al., "The 'IMPACT Super-Simulation' project for exploring NPP fundamental phenomena", paper presented at 2nd CSNI Specialist Mtg on Simulators and Plant Analysers, Espoo, 1997.
[IV–40] GAUVAIN, J., et al., ESCADRE Mod. 1.0: JERICHO: Reactor Containment Thermal Hydraulics during a Severe Accident: Reference Document, Rep. IPSN/DRS/SEMAR/96-06, Institut de Protection et de Sûreté Nucléaire, Paris (1996).
[IV–41] DELAVAL, M., et al., ESTER 1.0 Manual (Vols 1–4), Rep. EUR 16307/(1–4) EN, CEC, Brussels (1996).
[IV–42] PLYS, M.G., et al., "MAAP 4 model and validation status", paper presented at 2nd Int. Conf. on Nuclear Engineering, San Francisco, 1993.
[IV–43] SUMMERS, R.M., et al., MELCOR Computer Code Manuals, Primer and User's Guide, Version 1.8.3, Rep. NUREG/CR-6119, SAND93-2185, US Govt Printing Office, Washington, DC (1994).
[IV–44] KAJIMOTO, M., et al., "Development of THALES-2, a computer code for coupled thermal hydraulics and fission product transport analysis for severe accidents at LWRs and its application to analysis of fission product revaporization phenomena", paper presented at Int. Top. Mtg on Safety of Thermal Reactors, Portland, 1991.

# CONTRIBUTORS TO DRAFTING AND REVIEW

| | |
|---|---|
| Allison, C. | Innovative Systems Software, United States of America |
| Balabanov, E. | ENPRO CONSULT Ltd, Bulgaria |
| D'Auria, F. | University of Pisa, Italy |
| Jankowski, M. | International Atomic Energy Agency |
| Mišák, J. | International Atomic Energy Agency |
| Salvatores, S. | Electricité de France, France |
| Snell, V. | Atomic Energy of Canada Ltd, Canada |

**Technical Commitee Meeting**

Vienna, Austria: 30 August–3 September 1999