IAEA-TECDOC-1332

Safety margins of operating reactors

Analysis of uncertainties and implications for decision making

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

January 2003

The originating Section of this publication in the IAEA was:

Safety Assessment Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

SAFETY MARGINS OF OPERATING REACTORS:
ANALYSIS OF UNCERTAINTIES AND IMPLICATIONS FOR DECISION MAKING

IAEA, VIENNA, 2003
IAEA-TECDOC-1332
ISBN 92–0–118102–7
ISSN 1011–4289

Printed by the IAEA in Austria
January 2003

FOREWORD

Maintaining safety in the design and operation of nuclear power plants (NPPs) is a very important task under the conditions of a challenging environment, affected by the deregulated electricity market and implementation of risk informed regulations. In Member States, advanced computer codes are widely used as safety analysis tools in the framework of licensing of new NPP projects, safety upgrading programmes of existing NPPs, periodic safety reviews, renewal of operating licences, use of the safety margins for reactor power uprating, better utilization of nuclear fuel and higher operational flexibility, for justification of lifetime extensions, development of new emergency operating procedures, analysis of operational events, and development of accident management programmes.

The issue of inadequate quality of safety analysis is becoming important due to a general tendency to use advanced tools for better establishment and utilization of safety margins, while the existence of such margins assure that NPPs operate safely in all modes of operation and at all times. The most important safety margins relate to physical barriers against release of radioactive material, such as fuel matrix and fuel cladding, reactor coolant system boundary, and the containment. Typically, safety margins are determined with use of computational tools for safety analysis. Advanced best estimate computer codes are suggested e.g. in the IAEA Safety Guide on Safety Assessment and Verification for Nuclear Power Plants to be used for current safety analysis. Such computer codes require their careful application to avoid unjustified reduction in robustness of the reactor safety. The issue of uncertainties in safety analyses and their impact on evaluation of safety margins is addressed in a number of IAEA guidance documents, in particular in the Safety Report on Accident Analysis for Nuclear Power Plants. It is also discussed in various technical meetings and workshops devoted to this area.

The current report presents the results of a Technical Committee Meeting on Safety Margins of Operating Reactors and Implications for Decision Making including Considerations of Uncertainties of Analyses, held in Vienna, 15–19 October 2001. In this meeting specific topics related to the safety margins and their implications for decision-making were presented and discussed.

The IAEA officer responsible for this publication was M. Dusic of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

This publication has been prepared from the original material as submitted by the authors. The views expressed do not necessarily reflect those of the IAEA, the governments of the nominating Member States or the nominating organizations.

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

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

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

CONTENTS

1. INTRODUCTION

The safety margin of operating reactors is defined as the difference or ratio in physical units between the limiting value of an assigned parameter the surpassing of which leads to the failure of a system or component, and the actual value of that parameter in the plant. The existence of such margins assure that nuclear power plants (NPPs) operate safely in all modes of operation and at all times. The most important safety margins relate to physical barriers against release of radioactive material, such as fuel matrix and fuel cladding (typical limited values are departure from nucleate boiling ratio — DNBR, fuel temperature, fuel enthalpy, clad temperature, clad strain, clad oxidation), RCS boundary (pressure, stress, material condition), containment (pressure, temperature) and surrounding public dose. In many cases, both the limiting value and actual value are not known precisely, i.e. the safety margin cannot be quantified precisely. Therefore, for practical purposes, the safety margin is usually understood as the difference in physical units between the regulatory acceptance criteria and the results provided by the calculation of the relevant plant parameter. Further on in this document the "safety margin" term is used in this sense. Consequently, reducing the safety margin to zero (e.g. by approaching the maximum clad temperature of 1200°C) does not necessarily mean that the safety limit is reached. For example, the safety limit for fuel rods would be a coolable geometry. Calculations by complex computer codes are used to assess the values of safety margins. For this purpose a best estimate or a conservative approach is used.

The limiting value is generally referred as the safety limit or the acceptance criterion. The safety limits are limits for which plant is designed based on accepted codes and standards. The acceptance criteria are the criteria stipulated by the regulatory body based on national requirements and international norms for parameters relevant to the anticipated operational occurrences (AOOs), design basis accidents (DBAs), changes or phenomenon under considerations. The regulatory acceptance criteria could be more restrictive or same as safety limits depending on the national policy. For the purpose of evaluating safety margins, regulatory acceptance criteria should be taken as reference. Depending on the parameters and events considered in the evaluation of safety margins, regulatory body may specify requirements of the minimum safety margin.

In the past the margins to acceptance criteria have been determined by conservative evaluation model calculations. During the recent years an increasing tendency in computational reactor safety analysis is to replace these conservative calculations by "best estimate" or "realistic" calculations. In case of best estimate calculations it is necessary to supplement an uncertainty analysis of the code results when determining the safety margin. A prerequisite for this approach is, however, that qualified computer codes are available which are validated by pre- and post-test calculations of appropriate experiments, experiences from other plants and/or benchmark calculations on national and international levels.

The Technical Specifications of a NPP are provided to ensure that the plant operates in a manner with acceptable level of protection for the health and safety of the public. The bases of technical specifications define or address safety margins wherever possible and practicable. When proposing changes to design, test or procedure, it should be determined, if it would affect in any way, the safety margins. It is important to determine by calculational analyses at least the direction of the margin change (i.e. increasing or decreasing), before a decision is made on proposed changes.

Both improving analytical methods and updating plant equipment can increase margin. Once this increased margin is identified, some of the increase can be used to improve plant

performance. It is recognised that every numerical calculation used in safety assessment involves uncertainties, which are taken into consideration when defining minimum safety margins. It is these uncertainties, which can be reduced by applying better models, and methods, which in turn give more flexibility for the decision makers to propose or accept changes within the regulatory acceptance criteria. There are several examples when use of more advanced computational tools could allow increase of NPP power without any change of regulatory acceptance criteria.

Another trend around the world is to reduce barriers to trade and countries are developing market driven economics with open, competitive global trading. This trend is also seen in electricity supply industries, which results in an increased pressure to minimise the cost of production and to maximise outputs of the operating plants. These goals can be achieved by technical measures, such as power up-rating, increase of maximum fuel linear heat generation rate, optimisation of fuel management with the use of high burn-ups, use of mixed (i.e. U and Pu) oxide (MOX) fuel or use of mixed cores. Such plant modifications require an in-depth safety analysis to evaluate the possible safety impact. The analysis has to consider all the consequences of the plant modifications with respect to the margins existing under normal plant operation, loss of coolant accident (LOCA) conditions, transients (main steam line break, ATWS, station blackout, reactivity initiated accidents), and shutdown transients. The analysis must consider the core characteristics and the plant behaviour, taking into account the operability of the systems (e.g. cooling systems, electric power, heat sinks) including computer based systems with environmental effects, the reactor protection system set points, instrumentation with their sensitivities/ error band and operator actions.

The current report presents the result of the Technical Committee Meeting where specific topics related to the safety margins and their implications for decision-making were presented and discussed. The report comprises the following items:

- Capabilities of computer codes to accurately model reactor systems and phenomena (conservative vs. best estimate approach, evaluation of uncertainties, code assessment, user influence)

- Methods for safety margin evaluations for various NPP components and systems (methods and approaches, regulatory criteria, basis for decision making)

- Use of safety margins in operation and modifications of NPPs (results of analyses performed, typical limiting components, range of possible power uprating or increased operational flexibility, licensing aspects)

The Annex compiles individual papers submitted by the participants.

2. CAPABILITIES OF THERMAL HYDRAULIC COMPUTER CODES INCLUDING THE EVALUATION OF UNCERTAINTIES

2.1. Current status of widely used computer codes

2.1.1. General classification of computer codes, regarding uncertainty

The following definitions are used here:

Best Estimate (BE) code — a code which:

- is free of deliberate pessimism regarding selected acceptance criteria
- contains sufficiently detailed models to describe the relevant processes

Best Estimate (BE) analysis — accident analysis which:

- is free of deliberate pessimism regarding selected acceptance criteria
- uses a best-estimate code
- includes Uncertainty Analysis

Conservative code — a code which:

- has deliberate pessimism regarding selected acceptance criteria
- contains simplified models to describe the relevant processes

Conservative analysis — accident analysis which:

- has deliberate pessimism regarding selected acceptance criteria
- uses a conservative code and conservative initial and boundary conditions
- no separate treatment of uncertainties

2.1.2. List of major contemporary thermal hydraulic computer codes

There currently exist many complex codes used extensively for safety analyses of various designs of NPPs. The following thermal hydraulic codes have found wide international recognition:

BWR–PWR: ATHLET, CATHARE, RELAP5, TRAC, SCDAP,…
CANDU: CATHENA, TUF, RELAP5,…
Vendor specific codes: FRAMATOME ANP (former SIEMENS/KWU), WESTINGHOUSE, GIDROPRESS, etc.

2.1.3. Validation of codes

For most of the above listed codes qualitative validation has already been performed to a satisfactory extent. This has been achieved by comparing predictions of computer codes and models against experiments (SET) (ITF), recorded plant transients and/or benchmark calculations on national and international levels.

2.1.4. Evaluation of uncertainties

For quantitative validation of codes it is necessary to evaluate the uncertainty of the results from a complex set of calculations within a particular task (e.g. SAR for a given NPP). The main commonly recognised contributors to uncertainty of the results are described in the following table:

Contributors to the uncertainty of results	Uncertainty
code specific:	
• computational tools & numerical methods	• quantifiable in general terms
• physical models of separate phenomena	• quantifiable upon SET results
• geometry of the plant, represented by a set of interconnected volumes and structures	• partially quantifiable upon ITF results
plant data specific:	
• discrepancies between documents, presenting plant parameters, and real plant; • tolerances of plant parameters	• quantifiable by results of on-site checks and original design data
user specific:	
• insufficient modelling of the plant in the input deck	• quantifiable upon results from sensitivity studies and recorded plant transients or experiments
• inadequate assumptions for the Boundary & Initial Conditions (BIC)	• quantifiable upon results from sensitivity studies and recorded plant transients or experiments
• QA at code running and documenting	• difficult to quantify
Total uncertainty of results	**Quantifiable in general terms**

2.1.5. Conclusions of part 1: "Current status of widely used thermal hydraulic computer codes"

C1: State of the art codes generally allow reliable simulation of accidents and transients.

C2: Performing uncertainty evaluation with the state of the art methods and computational tools requires extremely **large amounts of time and resources** for the achievement of justifiable results.

C3: The currently proposed and applied uncertainty evaluation techniques (US regulatory guides, OECD reports) are not yet integrated in the licensing process of many countries.

C4: Methods and tools should be developed further in order to make possible the evaluation of the (total) uncertainty within reasonable time and resources limits.

Further **development** could be recommended in the following **fields**:

- evaluation and reduction of uncertainty in complex codes
- evaluation of experimental and plant data uncertainty (measurement errors)

- internationally tested set of methodologies for best estimate and uncertainty evaluation in NPP safety analysis
- computer tools for automated input preparation, performance of multiple code runs and statistic treatment of the results during uncertainty evaluation
- methodologies for accounting of scaling effects/extrapolation of code predictions beyond available experimental data.

C5: International efforts (ISP and similar) should be continued and extended to a larger number of code users with the purpose of "user effect" quantification.

2.2. Conservative versus best estimate approach

The ways to approach safety analysis for licensing purpose can be roughly summarised as follows:

Applied codes	Input & BIC (boundary and initial conditions)	Assumptions on systems availability	Approach
Conservative codes	Conservative input	Conservative assumptions	Deterministic*
Best estimate (realistic) codes	Conservative input	Conservative assumptions	Deterministic
Best estimate codes + Uncertainty	Realistic input + Uncertainty	Conservative assumptions	Deterministic
Best estimate codes + Uncertainty	Realistic input + Uncertainty	PSA-based assumptions	Deterministic + probabilistic

- *The approach, defined as "deterministic" includes implicitly some probabilistic evaluations for the applied conservative values, especially when their definition is based on engineering judgement or practical experience.*

Current licensing practice in many countries consists of using conservative BIC and assumptions as input for a best estimate or realistic code, as shown in the second line in the table above. It is believed that in this way all other uncertainties (e.g. code uncertainties, user effects, etc.) are adequately covered.

The Best-estimate analyses for licensing purposes (line 3 in the table above) are inherently deterministic. Therefore, such analyses must include the following BIC assumptions:

- Single failure in the Critical (Most Necessary) Safety System
- Additional failures — if required by the national regulations
- Actions of the Normal Operation Systems should not be taken into account if they affect the transient development in a positive way
- Plant parameters: measured values, decay-heat curve, fuel thermal conductivity, ECCS flow-rates, pellet-cladding gap size, containment state etc. — should be assumed **nominal**

Consequently, the uncertainty evaluation of such analyses:

- must not include variations in the assumed functioning of the Critical Safety System
- must not include variations in the assumed functioning of the Normal Operation Systems
- must evaluate or bound uncertainties due to:
  - plant parameters: measuring errors, decay heat curve, fuel thermal conductivity, ECCS flow-rates, pellet-cladding gap width etc.
  - nodalisation and other user effects
  - computational uncertainty
  - other sources of uncertainty.

In the full BE approach (line 4 in the table above) the BE values of BIC together with their uncertainties are used to calculate a value for a key parameter and its frequency distribution. Next the other uncertainties (model and code uncertainty, user effects etc.) are determined–or at least a safe upper bound value defined-and added to the key parameter uncertainty.

In this way a best estimate (median) value and a value with sufficient probability and confidence for the key output parameter will be determined. The uncertainty value (UV) should be added to the key parameter median value (KPMV), and then KPMV+UV should be compared with the relevant acceptance criterion to define the safety margin. The uncertainty value UV should be numerically determined so that possible key parameter value is less than KPMV+UV with the probability 95% (or other figure if prescribed by national safety authority). However, these approaches may not be always practicable in the analysis in view of statement C2 in section Conclusions of part 1: "Current status of widely used thermal hydraulic computer codes.

3. METHODS FOR SAFETY MARGIN EVALUATION

3.1. Safety limits/margins

3.1.1. Safety limits/criteria, regulatory acceptance criteria

Safety Margins are the differences in physical units between the established safety limits/criteria of assigned parameters associated with failures or changes of a system or component or with a phenomenon under consideration, and the calculated values of those parameters. Safety limits may be the limiting value used in the design or established for plant operation. Safety limits are specified in the Technical Specifications for a NPP, which shall not be exceeded during normal operations including anticipated operational occurrences. The terminology safety criterion is generally associated with the assigned parameter for design basis accidents (DBAs). The values of acceptance limits or criteria are stipulated by national Regulatory Bodies, not to be exceeded during DBAs. The regulatory limits or criteria may be the same or more restrictive than what the plant is designed for. Therefore, for practical purposes, the safety margin is usually understood as the difference in physical units between the regulatory acceptance criteria and the results provided by the calculation of the relevant plant parameter. In this document the "safety margin" term is used in this sense. Consequently, reducing the safety margin to zero (e.g. by approaching the maximum clad temperature of 1200°C) does not necessarily mean that the safety limit is reached. For example, the safety limit for fuel rods would be a coolable geometry. Calculations by

complex computer codes are used to assess the values of safety margins. While arriving at the safety margins due considerations should be given for conservatism or the uncertainties in calculations depending on the methodology adopted for computation to assure adequate confidence level either quantitatively or qualitatively as acceptable to the Regulatory Body. The methodology to be followed requires use of the state of the art technology and assurance of the quality in the evaluation of safety margins.

Figure 1 illustrates safety margins:

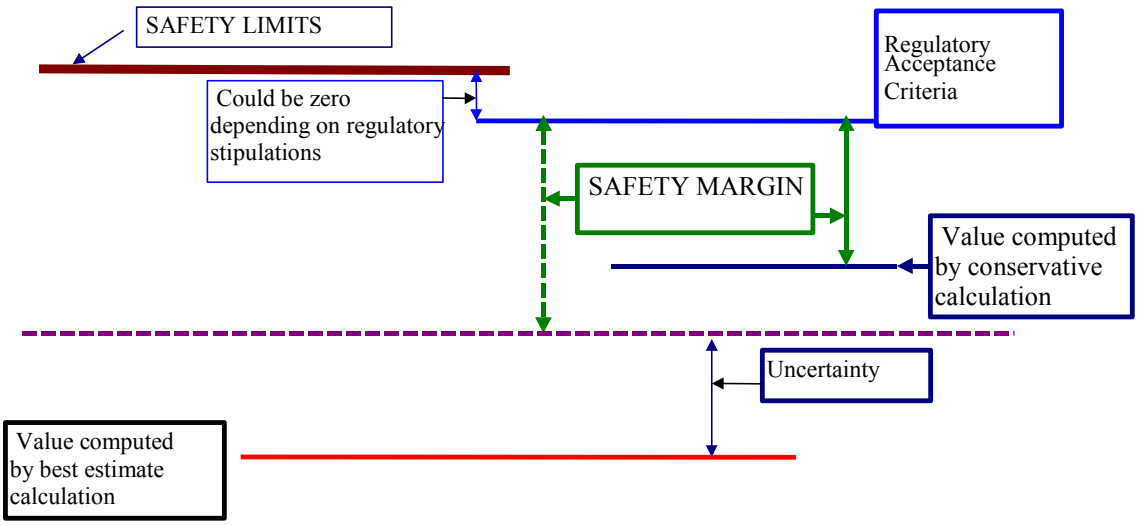


FIG. 1. Safety margins.

The parameter and regulatory acceptance criteria on the values of these parameters to be considered for assessment of safety margins will be governed by the type and characterisation of the failures (events), phenomena, and changes in the tests or procedures considered.

3.1.2. Deterministic safety limit

The parameters for deterministic safety margins include reactor coolant system pressure, minimum shut down margins, linear heat generation rate of fuel, fuel temperatures, fuel clad temperatures, departure from nucleate boiling ratio, fuel enthalpy, fuel clad strain and extent of oxidation, percentage of fuel failure, hydrogen generation, containment pressure and temperature, and radiation dose to plant personnel and the public. The safety limits are generally fixed as per international standards and accepted by national regulatory bodies as well. For LOCA design basis accident conditions, the regulatory criteria are for example:

- Peak clad temperature (1200°C)
- Maximum clad oxidation (17% of clad thickness)
- Maximum hydrogen generation (not to exceed deflagration or detonation limits for containment integrity)
- Coolable geometry of core

Using systematic procedures during transient and accident analysis of a NPP it is possible to transfer primary safety limits to a set of secondary physical parameters (secondary limits, such as subchannel outlet temperature, etc.), which can be measured directly or can be controlled through regular reload calculations.

3.1.3. Probabilistic safety target

Although emphasis is more focused on deterministic evaluation of safety margins, current international trend requires that the safety margins be evaluated with probabilistic safety analysis (PSA) as well, to support and supplement deterministic analysis, technical judgement and experiences to arrive at risk informed decisions.

The probabilistic safety margins may be defined as the difference between the established probabilistic safety targets acceptable to the regulatory body and the calculated value of the risk parameter taking into account uncertainties in failure data, modelling of common cause failures, human actions etc. and other uncertainties in knowledge. Presently, some countries rely heavily on PSA insights. If regulatory decisions (risk based decisions) are based solely on PSA results, then these probabilistic targets should be termed as probabilistic safety criteria (PSC).

The risk parameters considered for evaluations of probabilistic safety margins include risk importance measures of components, unavailability of safety systems, core damage frequency (CDF), change in CDF, radioactive release probability, individual risk of fatality and probability of societal loss considering all the three levels of PSAs.

Figure 2 below represents probabilistic safety margins:

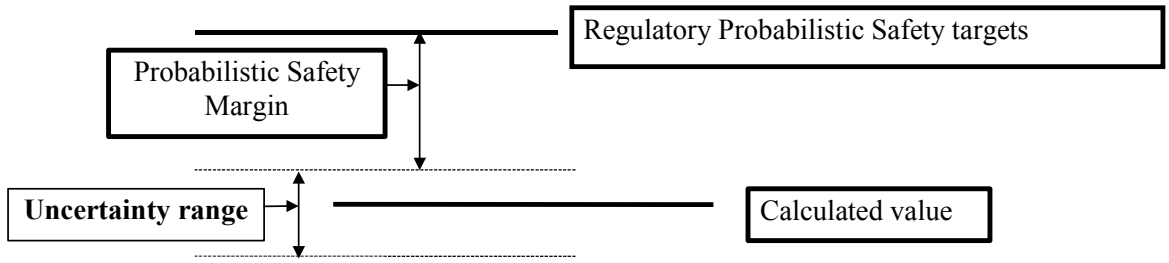


FIG. 2. Probabilistic safety margins.

The list below gives some regulatory Probabilistic safety targets [1, 2]:

- Shut down system unavailability (≤ 1E – 6 per demand)
- Engineered safety systems unavailability (≤ 1E – 3 per demand)
- Core damage frequency (≤ 1E – 5/Reactor-Year (R-Y))
- Probability for large radioactivity release (≤ 1E – 6/R-Y)
- Individual risk of fatality (≤ 1E – 6/R-Y)

It should be noted that these probabilistic safety targets might be different dependent on regulatory bodies of different countries.

3.1.4. Qualitative assessment and safety margin

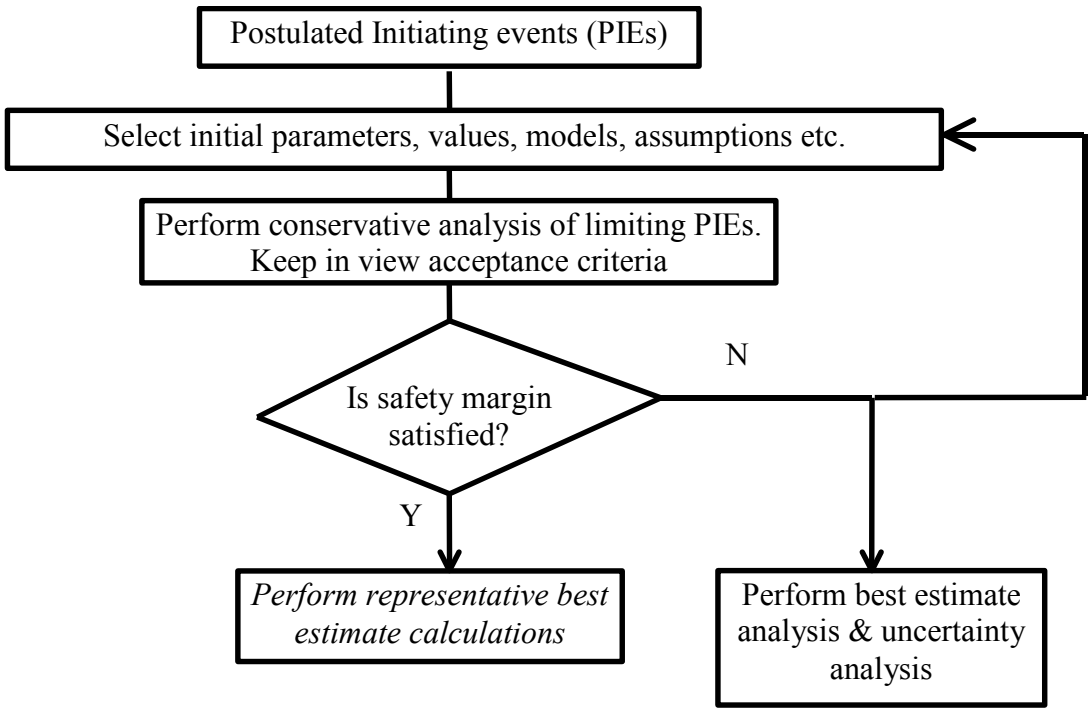
For every failure or phenomenon or change in tests or procedures of safety significance under considerations, it may not be possible to calculate the safety margin with state of the art technology available. This problem is usually solved by demonstrating either qualitatively or quantitatively, that those situations are adequately covered by the set of design basis transients

and that they do not produce an unacceptable increase in the usual risk indicators. In those cases where the exclusive use of qualitative arguments demonstrates that the safety margin exists, the calculations may be avoided (not the demonstration).

3.2. Approaches

3.2.1. Conservative estimate

Safety analysis should assure that the safety margins are defined and evaluated for each applicable regulatory acceptance criterion. Therefore, the safety analysis should include the list and analysis of all limiting initiating events keeping in view of regulatory acceptance criteria. The procedure could be as follows:



Conservative analysis should provide pessimistic estimate of the process relative to regulatory acceptance criteria under consideration and should be performed in accordance with existing guides. Best estimate code in combination with pessimistic assumptions can be used for conservative analysis with reduced conservatism. Each step in the conservative analysis, starting from selection of initiating events, should assure safety margins. Separate set of input parameters and separate accident scenarios should be defined conservatively for each acceptance criterion. Consequently, it may happen that the same initiating event can be analysed with different initial data and boundary conditions (failure assumption, accident scenario, etc.) depending on the acceptance criterion, which is under consideration.

Supplementary failures in redundancies in mitigating systems should be assumed in the analysis beyond single failure criteria if failure probabilities are considerable or required by Regulatory Body.

If safety margin is not satisfied in the conservative approach, the analysts may be demonstrated by the best estimate approach with uncertainty analysis to assure to be below the regulatory acceptance limit.

On the other hand, the secondary safety limits can be directly or indirectly measured or can be calculated using well based and generally accepted methods. The accuracy of measurement can be precisely defined; other tools of its determination (different codes) can be systematically validated. The measured or calculated parameter value may contain uncertainty, which should be well established to ensure that the parameter value is within the limiting value.

3.2.2. Best estimate with uncertainty analysis

The Code Scaling, Applicability and Uncertainty (CSAU) method was first developed and demonstrated investigating a large-break loss-of-coolant accident (LB LOCA) in 1989 by USNRC. Later several new methods were developed in the world:

- AEAW method (Atomic Energy Authority Winfrith)
- IPSN method (Institut de Protection et de Sûreté Nucléaire)
- GRS method (Gesellschaft für Anlagen-und Reaktorsicherheit)
- UMAE method (Uncertainty Methodology based on Accuracy Extrapolation)
- Tractebel method (Belgium)
- Limit value approach (ABB, USA), and a few others.

The first complete application of the UMAE method was carried out for a small break LOCA (6% area) in the Krsko nuclear power plant.

The uncertainty methods study group founded in the OECD/CSNI showed comparisons of five European Methods (the first four listed above plus ENUSA (Spain) method) in calculating uncertainty for ISP26 experiment.

In 1996, the Westinghouse best estimate LOCA licensing methodology based on WCOBRA/TRAC code and CSAU method was presented. Updates to about 20 plant's Final Safety Analysis Reports were performed by Westinghouse.

The CSAU approach was partly followed also in Japan for licensing analysis of boiling water reactor. General Electric (GE) method was used for Dodewaard BWR NPP upgrade renewal license in the Netherlands. Angra2 NPP licensing process in Brazil was performed by Framatome ANP (former Siemens/KWU), Germany applying CSAU.

Recently the methodology based upon CIAU (Code with Capability of Internal Assessment of Uncertainty) has been proposed [Ref. 3]. An example of CIAU application to WWER-440/230 licensing analysis is presented in the paper included in the Annex.

Another example of the practical use of uncertainty method (see Annex) is IJS application of CSAU to large-break and small-break LOCA in a two loop pressurised water reactor (PWR).

3.3. Initiating events (Transients/DBAs)

The selection of design basis transients is one of the main steps in the deterministic as well as probabilistic analysis. The ultimate goal of safety analysis is to evaluate the adequacy of plant protection and defence in depth so that safety functions are fully addressed. In the case of deterministic analysis, the focus is on magnitude of parameter and how effective are automatic protections and mitigative provisions.

Automatic protections are not designed to cope with everything. All the postulated initiating events (PIE) for the plant can be classified as "inside the design basis or beyond design basis" depending on whether they meet the design assumptions and requirements considered in the design of the plant.

The PIEs are subsets in the group of transients, for which the challenge to plant protection is maximum. The selection of the PIEs should ensure that the transients considered are enveloping/ severest when considered in the group of transients. In this sense, we say that the selection of design basis events should be comprehensive. The base transients should represent the most limiting conditions and, if any other transient is considered limiting, the analysis should be redone with this newly found limiting transient.

In parallel, the probabilistic analysis done with the set of initiating events, assumed initial conditions, and any assumptions made in fault tree and event tree levels, should assure with adequate confidence level that the calculated results of the parameter (viz. core damage frequency, large radio-activity release frequency etc.) are most probable value for the plant.

3.4. Quality assurance

3.4.1. General

Assurance of quality in the evaluations done by two different methods (approaches) namely the conservative analysis and best estimate with uncertainty analysis is essential. This requires that the choice of initial parameters and their values, assumptions, models are judicious, adequate validation of the codes, use of the state of the art technology, training and qualification of analysts and proper documentation. The variations in the results with the use of different codes and analyst performing the task should not be significant. The results before submission to the regulatory body should be peer reviewed.

3.4.2. Standardisation

Experiences show that safety margins evaluated with state of the art codes and experienced analysts vary significantly. This is one reason that uncertainty analysis is required for best estimate approach. Recently an uncertainty methods study [Ref. 4] comparison with five uncertainty methods (see chapter 0) was performed. Three of these methods used subjective probability distribution (GRS, Germany; IPSN, France; ENUSA, Spain), one (AEAT, UK) performed a bounding analysis and the fifth one (University Pisa, Italy) based on extrapolation from integral experiments did not use parameter uncertainties. The results showed the significant differences in the evaluations of cladding temperatures for the LSTF SB-CL-18, 5% cold leg small break LOCA experiment in the Japanese Large Scale Test Facility. Therefore, a need is recognised that efforts be made to standardise various steps involved in the evaluations to make the applications more practical and thereby acceptable to regulatory authorities.

4. UTILISING SAFETY MARGINS IN OPERATION AND MODIFICATIONS OF NPP

4.1. Role of PSA and deterministic analyses (DA) in plant modification

There are two basic types of plant modification with respect to its purpose: safety significant modification and cost reduction oriented modification within regulatory acceptance criteria.

4.1.1. Safety significant modification

Safety significant modifications are based either on findings from evaluation of existing safety margins or on PSA findings or on both. Safety significant modifications based on safety margin evaluation findings are usually carried out only in situation when safety margin for certain limit does not exist or is seriously challenged or is not accepted by regulator. In situation where safety margins exist and are accepted by regulator, safety significant modifications are usually based on PSA findings. Estimation and evaluation of current safety margins and possible changes in safety margins due to modification should take into account PSA findings and other analytical studies.

4.1.2. Cost reduction oriented modification

Cost reduction oriented modification should be evaluated with respect to safety margins and findings of PSA. Experience of some utilities show that even highly profitable modification like power up-rate can be carried out in such a way that it does not lead to significant decrease of current safety margins, and some safety margins can even be increased. In general, the possible decrease of some current safety margins due to cost reduction oriented modification can be accepted if affected safety margins stay at an acceptable level. Safety margins and their importance should be evaluated from global perspective that takes into account of possible radiological impact on plant personnel, the public and the environment.

In each case of modification in a NPP, it is necessary to analyse in details, steady state and dynamic characteristics of the plant including the neutron physical and thermal-hydraulic aspects, behaviour of materials of individual components and their operability and functional reliability. The analyses should take into account of appropriate values of input parameters, required settings of protective and control systems and interlocks, instrumentation with their sensitivities, acceptance criteria including limits and conditions for the safe operation, and relevant operating procedures etc.. After review and acceptance by the regulatory body, the results should be documented in the revised safety analysis report for the plant.

4.2. Evaluation of current safety margins and identification of weak points

The starting point for utilising safety margins for example in power uprating or other modifications is that the current safety margins and weak points are known and well identified. The bases for this are the existing licensing analyses. It depends on the modifications in question but normally the limiting cases are quite easily identified. Finding their weak points used to increase safety margins related to primary or secondary safety limits or to examine the possibility to re-evaluate these cases by uncertainty analysis to get less conservative safety factors/margins.

4.3. Measures to increase safety margins

If sufficient safety margins cannot be demonstrated, look out whether it is possible to fix safety criterion to a new value acceptable to regulatory body. It is clear that some primary safety criteria cannot be changed. Secondary limits such as burnup dependent linear heat rate limit can be changed, if new data from experiments and calculations with better codes show, that the goal behind the limit (limitation of fission gas release to limit pressure in the fuel rod and clad strength aspects) can still be reached.

Calculated safety margin can be improved also by screening out extra conservatism in the analyses. It may happen that using the latest state of the art codes improves the margins. The same applies also for input parameters. New knowledge may be available about a key input parameter, which allows to use a more realistic but still conservative value for the parameter.

It may be useful to use best estimate analysis supplemented by uncertainty analysis (UA) to show that adequate safety margin still exists after the plant modification. Development of UA-methods is going on as has been demonstrated in the papers of this Technical Committee Meeting. This approach may be very useful in the future, because computing power is no longer a limited factor. It is possible to run the required number of calculations with different input parameter values to be able to determine the uncertainty range of the results with sufficient confidence level (95%).

Screening out excess conservatism does not decrease safety. One can, however, demonstrate that the safety margins are larger than previously assumed. The new knowledge can be utilized, for example, by using more economic core loading patterns or by uprating the reactor power.

4.4. Some examples

Performing exclusively statistical uncertainty analysis may not reveal important phenomena like boron dilution effects depending on different break sizes and locations. One may miss the phenomenon by using only a few statistically selected break sizes, therefore a need for deterministic analyses remains.

Another example is the role of hydro-accumulators in LBLOCA. The hydro-accumulator parameters (pressure, water volume) are usually considered to be less important uncertain parameters compared to other uncertainties. However, substantial improvement in calculated safety margin has been obtained in the case of Loviisa NPP by changing these parameters. The change was based on engineering judgement and it's feasibility was proven by a wide spectrum of analyses. This is not "uncertainty of parameters" but "design optimisation".

Implementation of reactor trip additional initiators (primary pressure and temperature) may cope with some weak points of LOFA accident and thus increase safety margin (for example at V2 Bohunice NPP).

Another example, analyses during Level 1 PSA development for South-Ukrainian NPP has shown high practicality, technical and financial benefits. That has been reflected in understanding of necessity to adjust existing Unit Modernisation Program in the direction of further improvement of Reactor Installation safety and to develop a set of new measures,

some of which have not been so evident earlier, or could not be discovered without modern analytical tools for assessment of their contribution in WWER safety, such as a full set of Symptom Based EOP, Reactor Level and Coolant Voids Monitoring system, Plant General SPDS system.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Basic Safety Principles for Nuclear Power Plants, Safety Series No. 75-INSAG-3, IAEA,Vienna (1988).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant, Safety Series No. 106, IAEA, Vienna (1992).

[3] D'AURIA, F, GIANNOTTI, W., Development of code with capability of internal assessment of uncertainty, Nuclear technology, Vol.131, No.1, 159-196 (2000).

[4] WICKETT, T. et al., Report of the Uncertainty Methods Study for Advanced Best Estimate Thermal Hydraulic Code Applications, Volume 1 (Comparison) and Volume 2 (Report by the participating institutions), NEA/CSNI/R(97) 35 (1998).

Annex

PAPERS PRESENTED AT THE TECHNICAL COMMITTEE MEETING

FULFILLING THE REACTOR CORE LIMITATIONS WITH UPRATED POWER IN LOVIISA

M. ANTILA
Fortum Nuclear Services Ltd,
Vantaa, Finland

Abstract. In 1995 Fortum started a project for modernisation and power upgrading of the Loviisa NPP. This included gradual increase of the reactor thermal power up to 1500 MW (109%) and renovation of the steam turbines. The approach taken in the power uprating project was that the ultimate core limitations should remain unchanged. Room for power uprating was obtained by core loading pattern design and by screening out excess conservatism in the design calculations and on-line core monitoring. The core limitations and measures taken to fulfill the limitations with uprated power are discussed in this paper.

1. INTRODUCTION

In 1995 Fortum started a project for modernisation and power upgrading of the Loviisa NPP. This included gradual increase of the reactor thermal power up to 1500 MW (109%) and renovation of the steam turbines. As a result of a feasibility study it turned out that no major system or equipment modifications were required to reach 1500 MW power, which was thus selected as a target. The project, however, included certain improvements in the primary and safety systems to ensure plant safety.

At first stage the power upgrading to 1500 MW was realised within the ultimate core thermal and hydraulic limitations. Extra margin for increased reactor power was gained by flattening the core power distribution, which required a change from the low leakage loading pattern back towards the old out-in-in loading pattern. A partly low leakage loading pattern is currently used in the reduced cores (313 assemblies) of both units. The most strict core limitations were hot subchannel outlet boiling ($F_{\Delta h}$ limit), fuel assembly burnup and linear heat rate.

All transient and accident analyses and the Loviisa NPP Final Safety Analysis Report were revised in connection with the licensing process of the reactor power upgrading. Latest state of the art analysis tools and experience were utilised. Keeping the core thermal and hydraulic limitations unchanged resulted in that the effect of power uprating was very small in normal operation and transients. This is also true for accidents including LBLOCA particularly now that the optimization of the hydroaccumulator parameters has been completed.

A new operating license for 1500 MW reactor power was granted in April 1998 by the Finnish Government. The renovation of the steam turbines continued up to the year 2000. Some improvement in turbine efficiency was also achieved.

In this paper the experience gained in upgrading the power at Loviisa NPP is given concerning the reactor core limitations and measures taken to fulfil the core limits.

2. CORE LIMITATIONS AND THEIR BASIS

The most important core limitations are included in the plant technical specifications (TS) and they define the permissible initial states of the core, which are also assumed in the

safety analyses. The approach taken in the power uprating project was that the ultimate core limitations shall remain unchanged. This means that room for power uprating has to be obtained by core loading pattern design and by screening out excess conservatism in the design calculations and on-line core monitoring.

2.1. Linear heat rate

The local linear heat rate has an upper limit (325 W/cm) originating from the assumptions made in large break LOCA analysis. The limit is decreasing with burnup mainly to prevent excess fission gas release from the fuel pellets.

A safety factor of 1.12 is included in the calculated values to account for different uncertainties and tolerances. The upper limit is used in the transient and accident analyses including LBLOCA.

2.2. Subchannel outlet temperature

The hot subchannel outlet temperature is limited to bulk boiling, which means a temperature limit of 325^{o}C. The limit assures good DNB-margin against transients ($x < 0$ in initial state) and it also limits subcooled boiling in the core to an acceptable level.

A safety factor of 1.16 for the enthalpy rise is included in the calculated values to account for different uncertainties and tolerances. No coolant mixing between subchannels was previously assumed. Coolant mixing between adjacent fuel assemblies is not possible because of the assembly shroud tubes.

It turned out that the bulk-boiling limit is one of the most strict limits with respect to power uprating. The limit is difficult to fulfill with 1500 MW power especially for Loviisa-1, where the core flow is 5% less than for Loviisa-2. Power uprating requires also somewhat higher steam pressure and correspondingly 2 to 3^{o}C higher core inlet temperature.

2.3. DNB

The subchannel boiling limit assures that qood DNB-margin prevails in nominal operating conditions (initial states), where a typical DNB-ratio is about 3. No direct stedy state limit value has been imposed on DNB against transients. An initial state with hot subchannel being on boiling limit and conservative axial power distribution with linear heat rate being on the limit is assumed in the analyses. The 95/95 safety limit for DNB-ratio is 1.33, when using the Gidropress correlation. In addition the above-mentioned safety factor of 1.16 is used for local enthalpy rise and 1.12 for local heat flux.

2.4. Assembly power

In the fuel specification the assembly power limit is set to 6.4 MW. With 1500 MW reactor power this means an assembly power peaking factor (Kq) of 1.34. This is not, however, an ultimate safety limit in the sense of linear heat rate or DNB.

In analysing the LBLOCA it turned out that core power distribution has an effect on the maximum cladding temperature during the reflood phase.

2.5. Negative reactivity feedback

The combined reactivity feedback from core power shall always be negative. In practice it is required that even the reactivity coefficient of coolant temperature shall be negative in all critical states. This is confirmed by measuring the coefficient in BOC HZP for every new cycle.

In the safety anayses it is conservatively assumed that the coolant temperature coefficient is zero in HZP.

2.6. Reactivity control-by-control rods

The minimum requirement is 1% shut down margin down to 200^{o}C temperature with the most reactive control rod stuck in the upper position.

The lowest allowed position of the regulating group in critical state is limited as a function of reactor power. The purpose is to limit reactivity insertion potential in control rod ejection or control rod withdrawal accidents. Smoother power distribution is also favourable from the point of view of fuel pellet cladding mechanical interaction.

Conservative values are used in transient and accident analyses for control rod reactivity worths.

2.7. Reactivity control by soluble boron

The requirement is that with full boron concentration the reactor shall be at least 1% subcritical in all temperatures and burnup states without xenon and without control rods. During refuelling 5% subcriticality is required with any of the control rod fuel followers in the active core region.

2.8. Fuel burnup

The burnup limit for the Loviisa reactors imposed by the Finnish safety authority (STUK) has been 40 MWd/kgU for assembly average burnup. The purpose is to avoid unexpected fuel rod behaviour in accident situations (RIA, LOCA). At 1500 MW power and an with an equilibrium cycle length of 325 FPD in the Loviisa reduced core (313 assemblies) the average 3-batch discharge burnup of about 40 MWd/kgU would be reached. It was evident that the above burnup limitation cannot be met in the long run.

3. MEASURES TAKEN TO FULFILL THE LIMITATIONS WITH UPRATED POWER

3.1. Changing core loading principle

Extra margins for increased reactor power had to be gained by flattening the core power distribution [1]. This required a change from the full low-leakage loading pattern back towards the out-in-in loading pattern. A partly low-leakage basic alternative equilibrium cycle was designed to demonstrate the fulfilment of this requirement. Many additional variants were examined to in order to find out the possibilities to improve fuel cycle economy. The codes HEXBU-3D/MOD5 and ELSI-1440 were used. Basic cross sections were calculated with CASMO-HEX.

The partly low leakage basic alternative equilibrium cycle was designed for 1500 MW power. The target cycle length is 325 FPD. The annual fresh fuel feed consisted of 108 fixed and 12 fuel follower standard WWER-440 fuel assemblies with 3.6% enrichment.

In the partly low leakage loading pattern burnt fuel is placed in the outermost peripheral core locations to protect the pressure vessel weld from neutron irradiation in the critical direction.

At the moment we are in a transition phase towards full 3-batch loading pattern using 4.0% enriched fuel form TVEL and 3.7% enriched fuel from BNFL. A typical 3-batch equilibrium cycle core power distribution is given in Fig. 1.

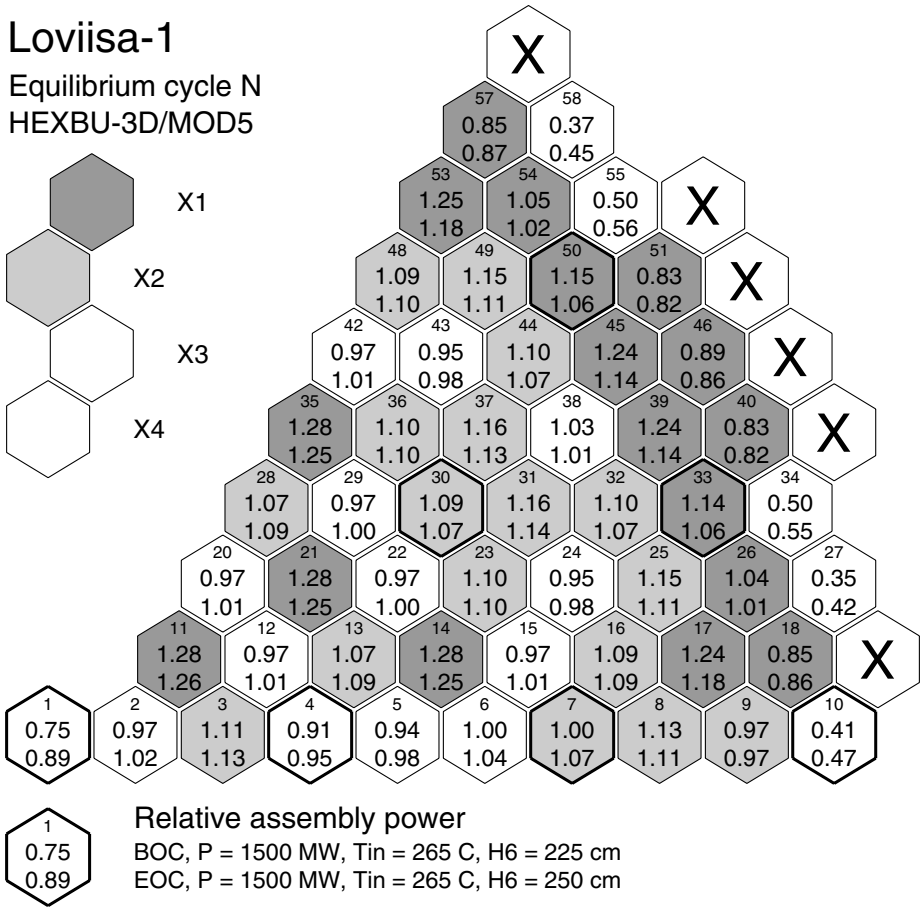


Figure 1. Core power distribution of 3-batch equilibrium cycle. X1 = first year fuel.

3.2. Increasing the burnup dependent part of linear heat rate limit

It was shown that it is possible to design the loading pattern such that the requirement of 325 W/cm set for the maximum linear heat generation rate can be met even with uprated power. In the beginning of cycle there is typically some per cent margin left to this limit, when the control rods are fully out of the core. In the end of cycle the margin was also scarce. That is why a re-analysis of the burnup dependent linear power limit was perfomed using the latest version of the ENIGMA code (instead of the erlier used GAPGON-THERMAL-2). The

goal of the analysis was to find a power history, which would result in approximately 1% fission gas release at the end of irradiation. As a result of the analysis an application was sent to and approved by STUK for increasing the burnup dependent part of the linear heat rate limit by 8% as compared to the earlier limit.

3.3. Taking into account assembly internal coolant mixing

The subchannel (Fig. 2) outlet temperature limit of 325^{o}C (bulk boiling limit) is difficult to fulfill with 1500 MW power especially for Loviisa-1, where the core flow is less than in the case of Loviisa-2. The subchannel outlet temperature limit is the most severe limitation with respect to 1500 MW power.

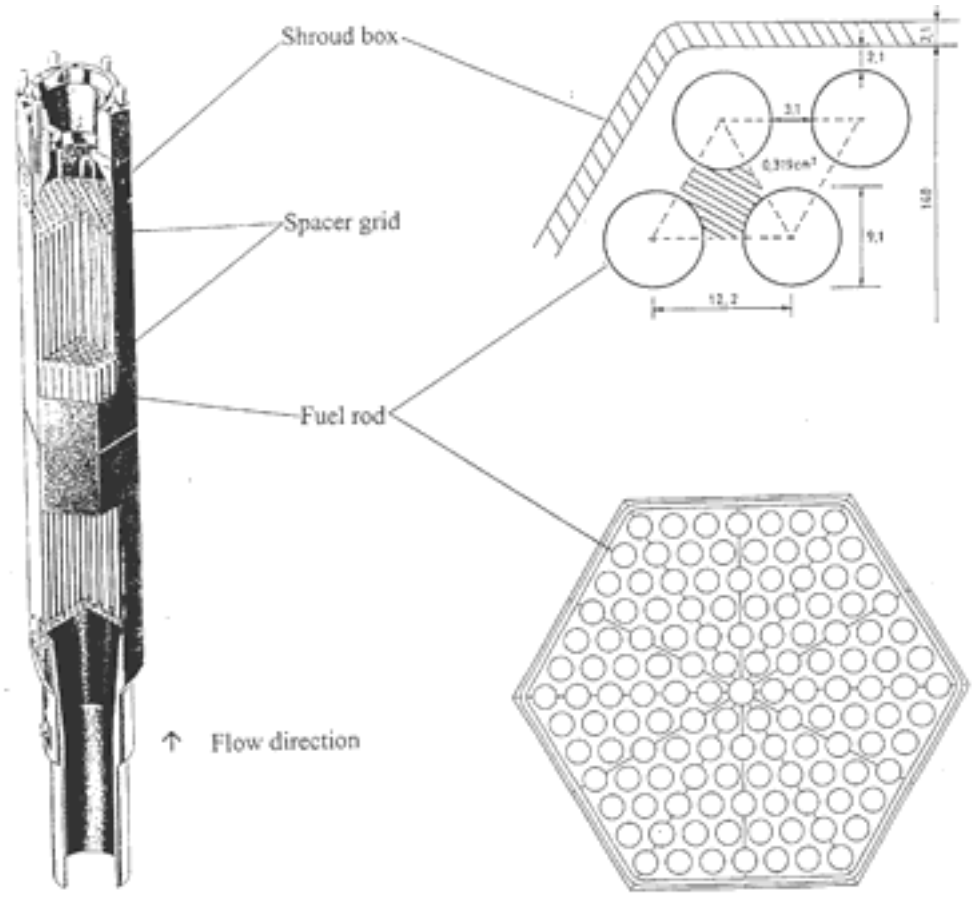


Figure 2. WWER-440 fuel assembly and subchannel.

Earlier the hot subchannel enthalpy rise peaking factor ($F_{\Delta h}$) was calculated conservatively assuming an isolated subchannel. According to detailed 3D CFD-calculations with the FLUENT tool package turbulent mixing and coolant flow redistribution inside the assembly shroud tend to smooth out the subchannel enthalpy rise peaking factor as compared to the isolated subchannel method. The calculated effect is in the order of 5...7% depending on the location of the assembly in the core.

The performed calculations were validated with experiments [2]. The experiments were carried out in cold state (20..60°C) for a real full scale fuel assembly with fuel pellets replaced with steel bars. A Laser Doppler Anemometry (LDA) was used for velocity and turbulence measurements. In LDA two laser beams with different angles are directed into the fuel assembly between the rods through a window made on the hexagonal shroud box of the test assembly. The small measuring volume is formed in the intersection volume of the two beams, where interference fringes are formed. Pulses of scattering light are got when the tracer particles in the fluid pass this volume. The local flow velocity is determined based on the frequency of the scattered light pulses. The measuring volume is moved to get velocity profiles inside the assembly. The main quantities measured inside the assembly were the local axial flow velocity and intensity of turbulence and in some points, also the crossflow velocity component. Several velocity and turbulence intensity profiles were measured on different levels in relation to the spacer grids. The effect of spacer grids on the flow field was studied extensively. Thousands of points were included in the measured data set in total.

The measurements were compared to the predictions of two CFD models based on the Fluent code. One model was developed particularly for this work (A) and the other (B) had been previously used in 3D flow and heat transfer analysis of the WWER-440 fuel assembly.

Figure 3 gives an example of measured and calculated axial velocity profiles from a diagonal penetrating into the fuel assembly between the rods at height 7th spacer grid 10 mm above the grid (downstream).

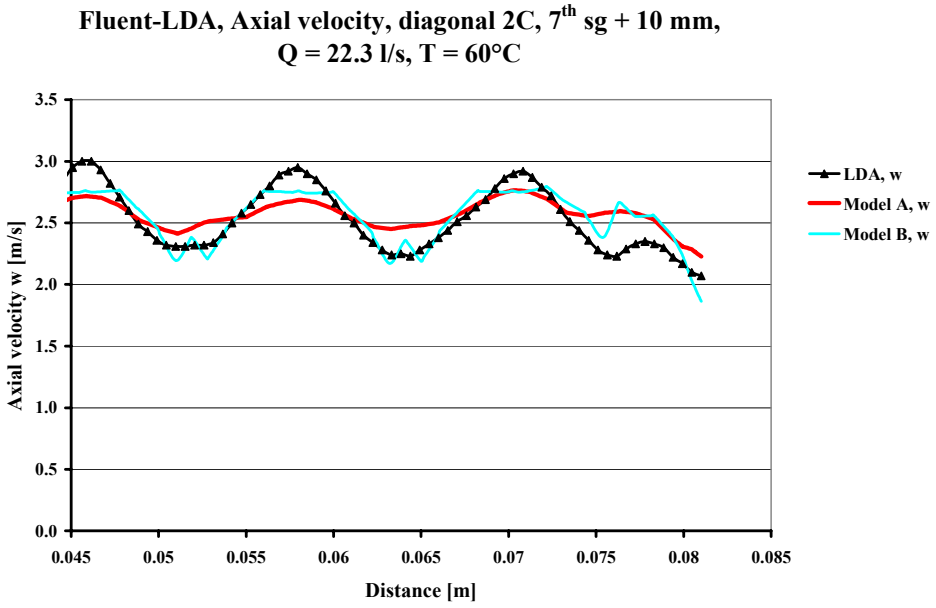


Figure 3. Measured and calculated axial velocity profiles from a horizontal diagonal penetrating into the fuel assembly between the rods at height 7th spacer grid + 10 mm.

The figure shows that at height 10 mm above the grid model A seems to underestimate the effect of spacer grid, the amplitude of the velocity profile is strongly underestimated just above the spacer grid. Both CFD models underestimate also the turbulence intensity near the spacer grid but already at height 20 mm they describe it with much better accuracy.

The LDA was found to be a very effective and reliable tool for measuring of the velocity and turbulence. The profiles measured from different windows were similar with

good accuracy. All measurements are also in harmony with calculated average velocity. It is concluded that the results of the work have created important knowledge of the flow field characteristics of the WWER-440 fuel assembly and have assisted in optimizing the CFD modeling of the assembly. Generally the CFD predictions were found to be satisfactory as compared to the LDA results, however some differences were also reported mainly related to the behaviour of turbulecne near the spacer grids. It is felt that the calculated results are on the conservative side.

STUK has accepted the use of the subchannel mixing credit, which is based on the application of the FLUENT code for analysis of coolant mixing in the WWER-440 fuel assembly. In spite of utilizing the mixing effect the subchannel boiling limit is now the most strict limit on core design and operation in Loviisa NPP. The alarm limit of the direct fuel assembly outlet temperature measurements (YQ30T) was consequently raised from the original 312^{o}C to 315^{o}C.

3.4. Improvements in LOCA response

LBLOCA is considered one of the most difficult licensing cases for the simulation codes to analyze. It was well known that LBLOCA is the most challenging accident case also in the power uprating project.

A detailed model of the Loviisa NPP was developed using the APROS Simulation Environment/3/. APROS is a computer independent code that supports several operating systems. It provides physical models, solution algorithms and generic components for use in different simulation systems for design, analysis and training purposes. With these tools full-scale modeling and simulation of power plant processes are available, including control and electrical systems. The thermal hydraulic models of APROS include one-dimensional three-, five- and six-equation flow models. One-dimensional solution of the heat conduction in the heat structures can be used together with each of the thermal-hydraulic models. All the thermal-hydraulic models are based on mass, energy and momentum conservation equations. The quantities to be solved in the model are pressures together with phasic velocities, void fractions and phasic enthalpies.

A thorough validation of the LBLOCA calculation model based on APROS was essential to be able to achieve reliability and credibility of the licensing analyses of the power uprating project. This process is described in more details in Ref. /4/. The APROS-model with 1-dimensional neutronics /5/ was used for other accident and transient analyses as well including ATWS. The coupled code HEXTRAN/SMABRE /6/ was used for cases, where 3D-neutronics description is essential.

The performed analyses showed that the results for hot rod cladding temperature for uprated power are in fact more favourable than the earlier results. The main explanation is that the maximum linear heat rate was kept unchanged (325 W/cm). Besides the linear heat rate the cladding temperature in the reflood phase is sensitive to the thermo-hydraulic behaviour of the circuit and core, which in turn depends on the safety system configuration and core power distribution. During the work it turned out that even more favourable results could be got by optimizing the hydroaccumulator water content and pressure. There is no ultimate uncertainty in these parameters as such but the sensitivity was revealed by engineering judgement. The pressure was reduced from 54 bar to 35 bar and the water inventory was increased from 40 m^3 to 50 m^3. Sensitivity of the results on core power distribution and hot assembly power peaking factor (K_q) was also examined. It turned out that the effect of loading pattern was significantly damped when new hydroaccumulator

parameters are used. It can be concluded that assembly power is no longer a key parameter in this respect (Fig. 4). Maximum rod linear heat rate determines the peak cladding temperature, which occurs in the blow-down phase.

Figure 4 shows the main results for hot rod temperature as a function of time. Even with uprated power significant improvement and thus extra margin in LBLOCA response was obtained as a result of the work. This is partly due to improved analysis methods and partly due to hydroaccumulator parameter optimization, which has been completed at the plant in summer 2001. Low cladding temperature results were one argument for incresing the fuel burnup limit.

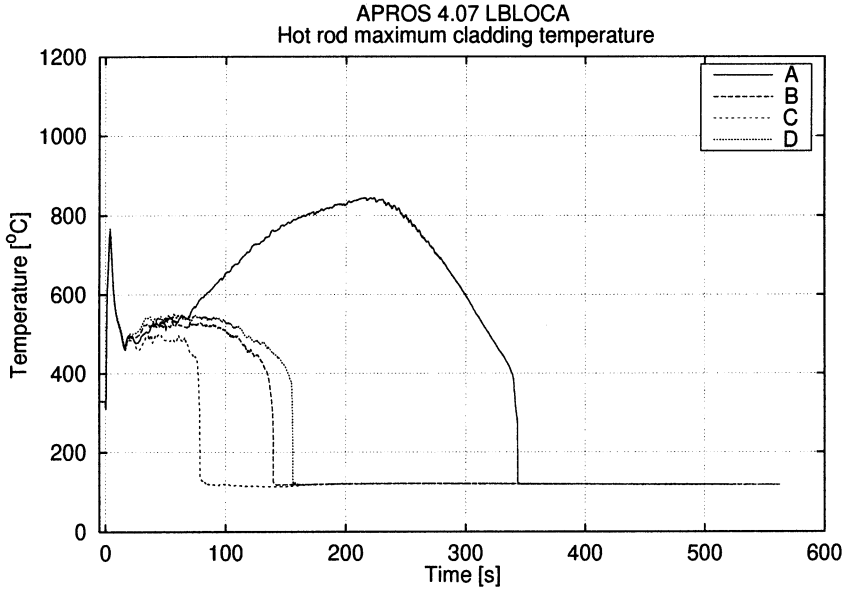


Figure 4. Hot rod maximum cladding temperature in LBLOCA. A = licensing case for power uprating, K_q = 1.33, B = optimized hydroaccumulator parameters, K_q = 1.33, C = as case B but K_q = 1.28, D = as B but K_q = 1.38 for single hot assembly.

3.5. Increasing fuel burnup limit

The burnup limit imposed by the safety authority STUK has been 40 MWd/kgU for the assembly average burnup. At 1500 MW power and an equilibrium cycle length of 325 FPD in the Loviisa reduced core (313 assemblies) the average 3-batch discharge burnup of about 40 MWd/kgU would be reached.

To make a full 3-batch loading pattern possible an application was sent to the safety authority for the approval of assembly burnup limit of 45 MWd/kg U, corresponding to maximum rod average burnup of 53 MWd/kgU. The application was mainly based on the results of a research programme contracted between Fortum (then Imatran Voima Oy) and the Russian fuel supplier. The programme included post-irradiation examination of 4 and 5 cycle fuel rods irradiated in the Kola plant and a series of transient tests and subsequent PIE of experimental rods made out of these fuel rods. Burnup of the test rods ranged up to 60 MWd/kgU. STUK has now made a positive decision on this matter. This decision was promoted by adjusting the hydroaccumulator water inventory and pressure, which resulted in low fuel cladding temperatures in LBLOCA.

3.6. Changing control rod insertion limit

The lowest allowed position (in TS) of the regulating group in HZP critical state was rised from 50 cm to 100 cm to to avoid heat transfer crisis (DNB) in control rod withdrawal transient without scram (ATWS) from low power initial state. The earlier limit would have caused heat transferr crisis and consequently high fuel cladding temperatures due to overpower already before the main coolant pumps trip from low steam generator level. By changing the limit the reactivity insertion potential was reduced to eliminate DNB.

3.7. Increasing full boron concentration

The equilibrium cycle calculations demonstrate that with the original full boron concentration of 2100 ppm (12 g/kg boric acid) the subcriticality of the reactor may not always be at least 1% negative reactivity if all control rods are fully removed from the core. To rule out any subcriticality problems even with extra long cycles the minimum full boric acid concentration was raised from the original 12 g/kg to 13 g/kg. The 5% subcriticality requirement during refuelling with any of the control rod fuel followers in the active core region can also be met.

3.8 Modernization of core monitoring system

On-line core supervision system (RESU) based on monitoring of local fuel limits has been in use at the Loviisa WWER-440 reactors already for more than twenty years. Power uprating and introduction of new fuel types gave rise to the latest improvements in the core supervision software system, which is now called RESU-98 /7/. The fast development of computing capacity was utilised in the modernisation. The in-core instrumentation system remained unchanged.

RESU-98 is an integral part of the Loviisa plant process computer system. Scanning of measurements, limit alarming, display of data and reporting is performed by utilising the process computer system software. The core performance calculation programs are run under the system like any other performance calculations, such as plant heat balance. Display formats are available for showing the direct in-core measurements (and their alarm limits) in digital form or on a core map and for showing distributions of calculated quantities on coloured core maps. Trend display formats including historical data for user defined calculated quantities or direct measurements can easily be defined by the operator. A covering collection of reports is available. Calculation of the core state is repeated automatically once an hour. The operator may activate core performance calculations at any time. Typical response time is a few seconds.

Evaluation of local fuel operating conditions is based on the fitted macroscopic 3D power distribution, assembly internal pin power distribution and assembly internal effective flow distribution. Linear heat rates, maximum fuel temperatures, maximum subchannel outlet temperatures and minimum DNB-margins are evaluated on local level. Fuel rod load changes are monitored by comparing the present power distribution to the previous power distribution. Alarm limits for the local in-core measurements are updated automatically once an hour after calculation of the core state.

The on-line core monitoring system RESU-98 is based on the use of validated codes. RESU-98 includes essentially the same computer codes that are used in reload planning. These are HEXBU-3D, which is a nodal code and ELSI-1440, which is used for pinpower reconstruction. Coolant mixing between subchannels inside the fuel assemblies is also taken

into account when evaluating the hot subchannel enthalpy rise and DNB-margin. The effect is in the order of 5...7% depending on the location of the assembly in the core. It is taken into account by a reconstruction method corresponding to the accuracy of the detailed CDF-calculations performed by using the FLUENT-code package. The on-line reconstruction method is very fast and still accurate.

The extensive in-core instrumentation including 132 local self powered neutron detectors of Rh-type and 192 fuel assembly outlet thermocouples are utilised to adjust the theoretical 3D-power distribution to get a best-estimate result. Interpretation of assembly outlet temperature measurements to assembly power values is possible because there are shroud tubes around the fuel assemblies. The neutron detector signals are interpreted into nodal fast flux values taking into account the properties of the surrounding fuel and the depletion of the detector. The Finnish Safety Authority (STUK) has given approval for the new RESU-98 system in August 1999. The system is in on-line use at the Loviisa NPP.

4. EXPERIENCE WITH UPRATED POWER

Up to now three full cycles with uprated power have been completed with both units. The reactor core peformace has been as expected. Particularly with LO1 the hot subchannel outlet temperature is still the most limiting parameter as can be seen in Fig. 5 for LO1 latest cycle 24.

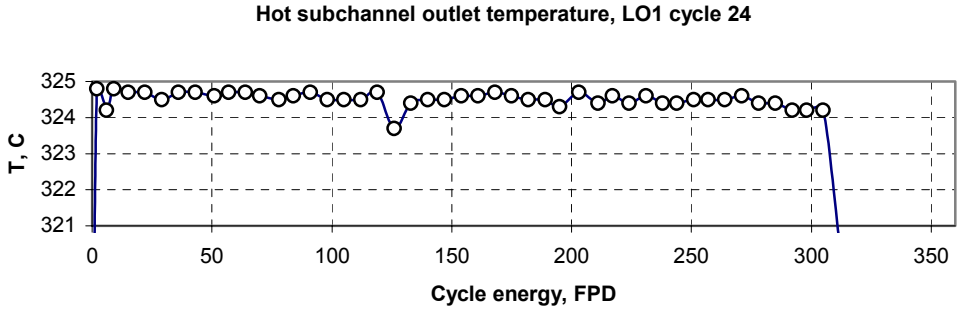


Figure 5. Hot subchannel outlet temperature as a function of cycle energy for Loviisa-1 cycle 24 according to the on-line core monitoring system. The limit is 325°C.

During refuelling in 2001 the hydroaccumulator parameters were adjusted. LO1 cycle 25 started with reload fuel from BNFL and LO2 cycle 22 with advanced fuel from TVEL. Now a transition phase towards a full 3-batch core is in progress. STUK has given approval for the assembly burnup limit of 45 MWd/kg U in September 2001.

5 SUMMARY AND CONCLUSIONS

In 1995 Fortum started a project for modernisation and power upgrading of the Loviisa NPP. This included gradual increase of the reactor thermal power up to 1500 MW (109%) and renovation of the steam turbines. The approach taken in the power uprating project was that the ultimate core limitations shall remain unchanged. Room for power uprating was obtained by core loading pattern design and by screening out excess conservatism in the design calculations and on-line core monitoring.

The burnup dependent part of the linear heat rate limit was increased by 8% as compared to the earlier limit.

Turbulent mixing and coolant flow redistribution inside the assembly shroud smoothen the subchannel enthalpy rise peaking factor as compared to the isolated subchannel method. According to detailed 3D CFD-calculations the effect was found to be in the order of 5...7% depending on the location of the assembly in the core. The calculations were validated with experiments carried out in cold state (20..60^{o}C) for a real full scale fuel assembly. A Laser Doppler Anemometry (LDA) was used for local velocity and turbulence measurements.

LBLOCA and other relevant analyses were performed using the detailed model of the Loviisa NPP developed using the APROS Simulation Environment. Conservative analysing practice was used. Typically uncertain key parameters were selected to be on the conservative side with 95% probability. According to the results the effect of power uprating was negligible on transients. The same is true also for accidens. The performed LBLOCA analyses showed that the results for hot rod cladding temperature for uprated power are in fact more favourable than the earlier results. This was mainly due to re-optimizing the hydroaccumulator water content and pressure. With new parameters the cladding temperature peak during the refill phase remains well below 600 ^{o} C. This result promoted also the acceptance of increased assembly burnup limit, which is now 45 MWd/kgU for assembly average burnup.

REFERENCES

[1] Antila, M., Siltanen, P., Experience gained in upgrading the power at Loviisa NPP, 8th AER Symposium on VVER Reactor Physics and Reactor Safety, 21-25 September 1998, Bystrice nad Pernstejnem, Czech Republic.

[2] Lestinen, V., Gango, P., Experimental and numerical studies of the flow field characteristics of VVER-440 fuel assembly, Ninth International Topical Meeting on Nuclear Reactor Thermal Hydraulics (NURETH-9), 3–8 October 1999, San Francisco, California.

[3] Porkholm, K., Honkoila,K., Nurmilaukas P., Kontio, H., APROS Multifunctional Simulator for Thermal and Nuclear Power Plants, Proceedings of World Congress on Systems Simulation ’97, September 1-3, 1997, Singapore, IEEE Singapore Section, Society for Computer Simulation Europe and Society for Computer Simulation International, pp. 504-508.

[4] Plit, H., Kontio, H., Kantee, H., Tuomisto, H., LBLOCA Analyses with APROS to improve Safety and Performance of Loviisa NPP, OECD-CSNI workshop on Advanced Thermal-Hydraulic and Neutronic Codes, 12-13 April 2000, Barcelona.

[5] Kuusisto, J., Antila, M., Description and validation of the 1-dimensional core model for the APROS analyzer of LOVIISA NPP, 6th AER Symposium on VVER Reactor Physics and Reactor Safety, 23-26 September 1996, Kirkkonummi, Finland.

[6] Hämäläinen, A.,Vanttola, T., Siltanen, P., Advanced Analysis of Steam Line Break with the Codes HEXTRAN and SMABRE for Loviisa NPP, OECD-CSNI workshop on Advanced Thermal-Hydraulic and Neutronic Codes, 12-13 April 2000, Barcelona.

[7] Antila, M., Kuusisto, J., Recent improvements in on-line core supervision at Loviisa NPP. OECD/NEA Workshop on Core Monitoring for Commercial Reactors, 4-5 October 1999, Stockholm, Sweden.

EVALUATION OF SAFETY MARGINS OF OPERATING REACTORS

H. GLAESER
Gesellschaft fuer Anlagen- und Reaktorsicherheit (GRS) mbH,
Garching, Germany

Abstract. The margins to acceptance criteria have been determined by conservative evaluation model calculations in the past. During the recent years an increasing interest in computational reactor safety analysis is to replace these conservative calculations by "best estimate" calculations supplemented by uncertainty analysis of the code results. Safety margin of operating reactors is defined as the difference in physical units between the critical value of an assigned parameter associated with the failure of a system or component or with a phenomenon and the actual value of that parameter. The most important safety margins relate to physical barriers against release of radioactive material. Margin can be increased by improving analytical methods or plant equipment. Once this increased margin is identified, some of the increase can be used to improve plant performance. Computer code calculations are used to assess the values of safety margins. For this purpose a best estimate or conservative calculation is used. In case of best estimate calculation it is necessary to determine the uncertainty band when determining the safety margin. A prerequisite for this approach is, however, that qualified computer codes are available which are validated by pre- and post-test calculations of appropriate experiments. Utilities intend to minimise the cost of production and to maximise outputs of the operating plants. These goals can be achieved by technical measures, such as power up-rating, increase of maximum fuel linear heat generation rate, optimisation of fuel management with the use of high burn-ups, use of mixed (i.e. U and Pu) oxide (MOX) fuel or use of mixed cores. Such plant modifications require an in-depth safety analysis to evaluate the possible safety impact. The analysis has to consider all the consequences of the plant modifications with respect to the margins existing. The analysis must consider the core characteristics and the plant behaviour, taking into account the capability of the systems (e.g. cooling systems, electric power, heat sinks) and the reactor protection system set points. The origin of margin evaluation came from LOCA. An approach to examine safety margins might be more general. The key issue in improving the plant operating performance is the accurate determination of the available plant margin. In relation to LOCA analysis margin can be characterised as the difference between calculated parameter values (e.g. peak fuel clad temperature, maximum reactor coolant system pressure, etc.) and the associated regulatory acceptance limit. Their determination includes considering the examining tools and methodologies (conservative versus best estimate approach), the applicability and quality of computer codes, the prediction capability and uncertainty evaluation, the acceptance criteria, and the accuracy of plant measurements.

1. INTRODUCTION

During the recent years an increasing interest in computational reactor safety analysis is to replace these conservative calculations by "best estimate" calculations supplemented by uncertainty analysis of the code results. In the past, margins to acceptance criteria have been determined by conservative evaluation model calculations. Margin can be increased by improving analytical methods or plant equipment. Once this increased margin is identified, some of the increase can be used to improve plant performance. A prerequisite for this approach is, however, that qualified computer codes are available which are validated by pre- and post-test calculations of appropriate experiments.

Another trend around the world is to reduce barriers to trade and countries are developing market driven economics with open, competitive global trading. This trend is also seen in electricity supply industries, which results in an increased pressure to minimise the cost of production and to maximise outputs of the operating plants. These goals can be achieved by technical measures, such as power up-rating, increase of maximum fuel linear heat generation rate, optimisation of fuel management with the use of high burn-ups, use of mixed (i.e. U and Pu) oxide (MOX) fuel or use of mixed cores. Such plant modifications require an in-depth safety analysis to evaluate the possible safety impact. The analysis has to consider all the consequences of the plant modifications with respect to the margins existing under normal plant operation, loss of coolant accident (LOCA) conditions, transients (main

steam line break, ATWS, station blackout, reactivity initiated accidents), and shutdown transients. The analysis must consider the core characteristics and the plant behaviour, taking into account the capability of the systems (e.g. cooling systems, electric power, heat sinks) and the reactor protection system set-points.

2. DEFINITION OF "PLANT MARGINS"

The key issue in improving the plant operating performance is the accurate determination of the available plant margin. Safety margin of operating reactors is defined as the difference in physical units between the critical value of an assigned parameter associated with the failure of a system or component or with a phenomenon and the actual value of that parameter. Such margins assure that nuclear power plants (NPPs) operate safely in all modes of operation and at all times. The most important safety margins relate to physical barriers against release of radioactive material. In relation to LOCA analysis margin can be characterised as the difference between calculated parameters (e.g. peak fuel clad temperature, clad strain, maximum reactor coolant system pressure and stress, containment pressure and temperature, etc.) and the associated regulatory acceptance limit.

The following physical parameters may be demonstrated to be below acceptance or design limits: Fuel rod performance (fuel clad temperature, fuel temperature, fuel enthalpy, clad strain, fuel clad failures, clad oxidation, departure of nucleate boiling — DNB, minimum critical power ratio — MCPR), reactor coolant system performance (pressure, flow, stress), and containment performance (peak pressure and temperature).

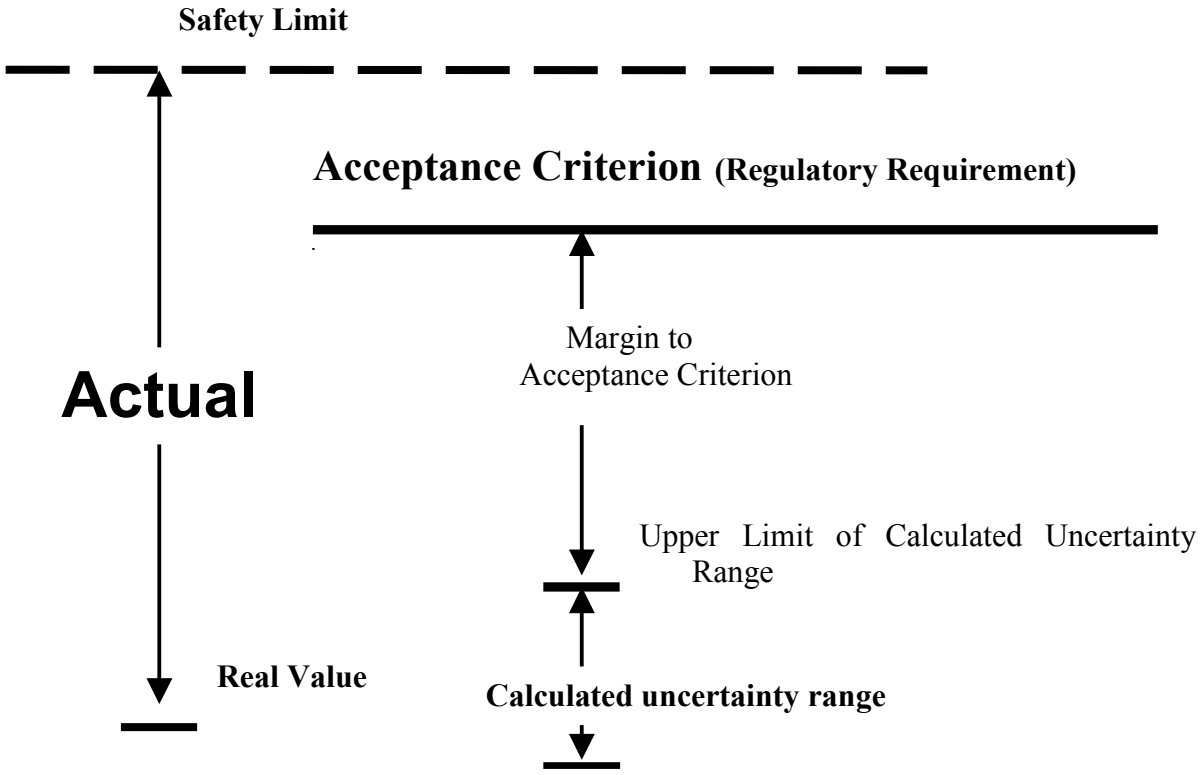


Figure 1. Margin illustration.

These margins are usually called “margin of safety”, e.g. in reference [17]. However, reducing the margin to an acceptance limit close to zero is not implying a close to zero reduction of the “safety margin” to zero. The term “safety margin” is here understood as margin to the safety limit. The safety limit is considered as coolable geometry (a rubble bed is considered not coolable). Usually, the design of a nuclear reactor plant is not based on the safety limit but on the regulatory acceptance limit, see figure 1. The safety margin can only be determined with some uncertainty, and would need a detailed investigation of fuel performance. Therefore, the plant margin may be called “margin to acceptance criterion”. This difference between safety margin and margin to acceptance criterion is typical for fuel performance, not for other areas.

Complex computer codes are used to determine the values of safety margins. For this purpose a best estimate calculation or a conservative calculation is performed. Using best estimate calculations requires to evaluate the uncertainty range of the calculation results for assessing the safety margin.

3. EXAMINING TOOLS AND METHODOLOGIES FOR SAFETY MARGIN EVALUATION (CONSERVATIVE VERSUS BEST ESTIMATE APPROACH)

The licensing requirements usually limit the core power and peak linear heat generation rates (LHGR) available to the designer. The licensing requirements also establish the minimum performance requirements of plant equipment and how the availability of plant equipment effects the plant system performance evaluations such as single failure criterion.

The reactor peak linear heat generation rate and total thermal power limits are established by reactor safety analysis including the loss of coolant accidents, anticipated transients which can lead to departure from nucleate boiling (DNB), and transients that lead to fuel melt.

In the past, the loss of coolant accident have limited the magnitude of peak LHGR which can be allowed in the plant. The design basis LOCA, along with reactivity control, is one of the cornerstones of nuclear power safety. The LOCA regulations were originally adopted in USA in 1974 after several years of development and interim criteria. They are documented in 10 CFR 50.46 and Appendix K [6]. While Appendix K is meant to apply to the spectrum of large and small break LOCA, its emphasis is clearly directed towards large breaks. Most typically, this is the break of a cold leg in a pressurised water reactor. It has indeed been applied to a spectrum of break sizes, including small breaks. These rules codified a rather prescriptive procedure for performing LOCA analysis. In view of existing uncertainties in the data and limitations in modelling, artificial conservatisms were introduced to various parts of the analysis.

After extensive research was carried out to reduce the uncertainties associated with LOCA analysis the acceptance criteria for emergency core cooling systems (ECCS) for light water nuclear power reactors (§ 50.46) was revised in 1988 to permit realistic analysis describing the behaviour of the reactor system during a LOCA. Comparisons to applicable experimental data must be made and uncertainties must be accounted for, so that, when the calculated ECCS cooling performance is compared to the acceptance criteria, there is a high level of probability that the criteria would not be exceeded [6]. A Regulatory Guide [16] describes models, correlations, data, model evaluation procedures, and methods that are acceptable to the NRC staff for meeting the requirements for a realistic or best-estimate calculation of ECCS performance during a LOCA and for estimating the uncertainty in that

calculation. Methods for including the uncertainty in the comparison of the calculation results to the acceptance criteria are also described in the Regulatory Guide. It is proposed to demonstrate that the criteria will not be exceeded with a probability of 95% or more.

Other countries have established efforts to quantify code uncertainty as well. An overview on utilisation of best estimate methodology in safety analysis and licensing in OECD/ CSNI member countries was compiled in 1996 [11]. A best estimate method including uncertainty evaluation was applied for e.g.:

- Doodeward BWR NPP upgrade renewal license in the Netherlands performed by GE, USA; GRS was advisor of the licensing authority "Gemeenschappelijke Kernenergiecentrale Nederland (GKN), 1993-1995
- Angra 2 NPP licensing process in Brazil performed by Framatome ANP (former Siemens), Germany; GRS was advisor of the Brazilian licensing authority "Comissao Nacional De Energia Nuclear (CNEN), 1998-1999
- Updates to about 20 plant's Final Safety Analysis Reports performed by Westinghouse (acceptance of methodology by USNRC after rigorous review spanning 3 years, over 550 requests for additional information)
- AP600 large break LOCA analysis performed by Westinghouse.

The analyses for PWRs were performed to investigate large break loss of coolant accidents.

A seminar on best estimate methods in thermal-hydraulic safety analysis was held on 29 June through 1 July 1998 in Ankara, Turkey, sponsored by the CSNI [13] The objective of the seminar was to review the insights from and the status of utilisation of best estimate methods in plant safety analysis needed in support to the licensing process.

An international meeting on "best estimate" methods in nuclear installation safety analysis (BE-2000) took place from 13 through 16 November 2000 in Washington, DC, USA [4] covering a broad spectrum of topics. It was pointed out that BE methods are just as likely to increase safety as to provide economic gains. The issue of BE methods uncertainties is not resolved yet. More attention should be paid to uncertainty of physical models. Also, there is a problem of definitions and nomenclature, which need to be standardised. However, a consensus that creation of an "effective" standard(s) for BE methods and applications is possible was not clear.

With the revision of the US rule, improved analysis methods with best estimate thermal hydraulic codes can now be used to calculate the LOCA. While the emergency core cooling system acceptance criteria have not changed, the method used to evaluate the reactor plant response for the postulated accident has changed which will result in additional LOCA margin for the utilities. Previous methods had imposed conservatism to either cover uncertainties or to simplify and reduce the event for the analysis. By employing the best estimate methodology, the additional conservatisms are removed and margin is generated.

4. ACCEPTANCE CRITERIA

Acceptance criteria are those values, established by Regulatory Authorities, to which the licensee is committed through its final safety analysis report (as updated), as the basis for acceptability of response to the postulated LOCA, transient or malfunction [17]. The LOCA design basis accident licensing criteria are:

1. Peak clad temperature (1200°C)
2. Maximum clad oxidation (17% of the total clad thickness before oxidation)
3. Maximum hydrogen generation (1% of the hypothetical amount that would be generated if all the metal in the clad cylinders surrounding the fuel, excluding the clad surrounding the plenum volume, were to react)
4. Coolable geometry
5. Long-term cooling.

These criteria were used by other national regulatory authorities, partly with some slight changes or additions.

A fuel safety criteria technical review has been performed by a PWG2 Task Force [18] Safety issues were identified and addressed which are connected with advanced fuel and core designs and operating strategies. At burnups above around 40 GWd/t, the oxidation rate of zircaloy increases significantly. Investigations have been performed and are continuing to clarify the oxidation process during normal operation and its effect to the brittleness of the remaining clad material, compared with the oxidation during the LOCA at higher temperatures [18]. The question whether the different oxidation process at LOCA temperatures should be accounted for when comparing against the 17% LOCA-limit is unsettled, and will hopefully be resolved from further experiments [18].

In view of further improvements of fuel design, notably to extend the burnup, fuel acceptance criteria should continue to be assessed with the support of experimental research under RIA and LOCA conditions [18]. Also, the analysis methods and modelling needs further improvement, with suitable validation against experimental data. Experimental data are also needed in specific areas in order to address unresolved issues. As an example, as highly oxidised clad may have different boiling characteristics as compared to fresh fuel, reliable data on the possible effect on critical heat flux would be required.

An examination of initial and boundary conditions to LOCA analysis with regard to the conservative requirements of Appendix K has been presented in [5]. It is intended to highlight some important basis of Appendix K requirements as well as possibilities to use different parameter values in best estimate analysis.

5. ACCURACY OF PLANT MEASUREMENTS

In order to evaluate safety margins the accuracy of reactor plant measurements may be important. This refers mainly to measure enthalpy flows, i.e. measuring the feed-water flow rate, feed-water flow temperature, and steam quality. The established accuracy of these measurements, for example, resulted in the requirement of Appendix K to assume that the reactor is operating at 102% of the licensed maximum power prior to the initiating event. A reduction of the 2% margin in power is discussed in the USA based on possibly improved measurement methods [5]. This reduction is not yet agreed internationally. Contrary arguments refer to ranges of the power limitation systems and non-zero measurement uncertainties.

6. APPLICABILITY AND QUALITY OF COMPUTER CODES

The use of “best estimate” computer codes is only acceptable if the codes are applicable to the accident scenario to be investigated. The code has to be fully qualified. This implies a demonstration of performed validation activity. The CSNI Validation Matrices [1],

[3], [15] may be a basis for this validation work. A challenge in the frame of code validation is the participation in International Standard Problems (ISPs) and benchmarks.

Specific areas for code improvements were identified during the OECD/CSNI Workshop on Transient Thermal-Hydraulic and Neutronic Code Requirements in Annapolis, November 1996[12]:

1. multi-field models
2. interfacial area transport model
3. multi-dimensional hydrodynamics
4. operation at low power/low flow
5. operation in presence of non-condensables
6. 3-D neutronics
7. low diffusive numerical methods
8. front (steep gradient) tracking.

In a follow-up workshop current and future applications of advanced thermal-hydraulic and neutronic codes were presented and discussed [14].

Computational fluid dynamics (CFD) programmes have a large potential for the detailed simulation of multi-dimensional flows. For one-phase flows, they are already applied successfully. In future, it will be state of the art to simulate two-phase flows with CFD programmes as well.

7. PREDICTION CAPABILITY AND UNCERTAINTY EVALUATION

The evaluation of the margin to acceptance criteria, e.g. the maximum fuel rod clad temperature, should be based on the upper limit of the calculated uncertainty range of clad temperatures, for example, see Figure 1. Uncertainty analysis is needed if useful conclusions are to be obtained from “best estimate” thermal-hydraulic codes, otherwise single values of unknown accuracy would be presented for comparison with limits for acceptance.

Methods have been developed and presented by research organisations, technical support organisations and vendors/utilities to quantify the uncertainty of computer code results [7], [8], [10], [19], [20].

A recent Uncertainty Methods Study (UMS) demonstrated the availability of various methods for the quantification of uncertainty [19]. Five different uncertainty methods and their applications have been compared. Four methods identify and combine input uncertainties. Three of these, the GRS-Germany, IPSN-France and ENUSA-Spain methods, use subjective probability distributions and one, the AEAT-UK method, performs a bounding analysis. Each method was used to calculate the uncertainty in specified code calculation results for the LSTF SB-CL-18 5% cold leg small break LOCA experiment in the Japanese Large Scale Test Facility (LSTF). The major differences between the predictions of clad temperature ranges by the methods came from the quantification of the input uncertainties, and consequently, the wideness of the uncertainty ranges and the choice of uncertain parameters. One of the methods, the Pisa (Italy) method, does not use parameter uncertainties, it is based on extrapolation from integral experiments. To use this method criteria on the code and experimental data base must be met. For the Pisa method differences come mainly from the optimisation of the nodalisation and from the different number of experiments investigated. Care must be taken to select suitable experimental and analytical information to

specify uncertainty distributions or to quantify the accuracy of code results. Statistical statements cannot be made, like probability of 95% or more that licensing criteria will not be exceeded.

A need is recognised to increase the effort towards harmonisation and practical applicability of these methods. An internal assessment of uncertainty in the codes is under investigation.

8. GERMAN PRACTICE IN UTILISATION OF BEST-ESTIMATE METHODOLOGY IN SAFETY ANALYSIS AND LICENSING

There are two kinds of conservative assumptions in performing safety analysis. The first one considers the limited availability of components and systems. Examples of German licensing requirements are single failure criterion, additional unavailability due to preventive maintenance, and its most unfavourable initial conditions. These assumptions have to be applied for all deterministic analyses.

The second kind of conservative assumption takes into account insufficient knowledge. Due to research and development programmes the knowledge increased. Consequently, corresponding recommendations of code models as well as conditions in the RSK-Guidelines (Reactor Safety Commission) allow latitude towards the application of best-estimate models and assumptions. An example is the recommendation to assume no residual water in the pressure vessel after blowdown during a large break loss of coolant accident at the beginning of the refill phase. After a big number of experiments have demonstrated that this assumption is not valid, it was no more applied. Flexibility to follow advances in safety technology and to transfer reliable results from research and development into code models and assumptions are allowed. The selection of recommendations of the RSK reflect the priority of large break loss of coolant accidents.

Rules and guidelines do not require an evaluation code with frozen conservative models in Germany. Safety rules and guidelines allow that deterministic thermal-hydraulic code analyses were performed using best estimate codes in the licensing processes. However, conservative initial and boundary conditions were applied for all analyses.

Parallel to the trend towards more realistic best-estimate calculations, methods for quantification of uncertainties of calculation results have been developed, tested and partly applied in Germany. Binding regulations for uncertainty evaluation do not exist. The former RSK together with the GPR (Groupe Permanent Réacteur), the French Reactor Safety Commission, recommended the use of realistic assumptions and models for the European Pressurised Water Reactor (EPR) safety demonstration. Compliance of the results with the existing licensing criteria has to be proven at high confidence level which means the explicit evaluation of the associated uncertainties. The committee did also allow the use of models and criteria according to the conservative approach as applied in the past. In the long term, however, the latter alternative is not preferable because it does not allow to utilise the high level of code validation.

Two methods for evaluation of uncertainties are available in Germany at present. The designer's method (Framatome ANP) follows essentially the CSAU (Code Scaling Applicability Uncertainty) method proposed by USNRC, but differs in the application of some steps [8]. The GRS method has been developed for application of future confirmatory analyses conducted as part of the safety assessment by expert organisations [9].

The formal regulation with respect to uncertainty evaluation in the licensing process is under discussion presently. A revision of the KTA-Standards (Nuclear Standards Committee) is in progress including best estimate analysis.

9. CONCLUSIONS

It has been stated that a great deal of communality of practices of safety analysis exist in OECD/ CSNI countries, although the details may differ. Methods to evaluate uncertainties in licensing procedures are not yet settled in most countries. An effort towards harmonisation and practical applicability of uncertainty methods would be beneficial.

REFERENCES

[1] AKSAN N., D'AURIA F., GLAESER H., POCHARD R., RICHARDS C., SJÖBERG A. Separate Effects Test Matrix for Thermal-Hydraulic Code Validation, a) Volume I: Phenomena Characterisation and Selection of Facilities and Tests, b) Volume II: Facility and Experiment Characteristics. NEA/CSNI/R(93)14/Part 1 and Part 2, Paris 1994.

[2] AKSAN N., D'AURIA F., GLAESER H., LILLINGTON, J., POCHARD R., SJÖBERG A. Evaluation of the Separate Effects Tests (SET) Validation Matrix. NEA/CSNI/R(96)16, November 1996.

[3] ANNUNZIATO A., GLAESER H., LILLINGTON J., MARSILI P., RENAULT C., SJÖBERG A. CSNI Integral Test Facility Validation Matrix for the Assessment of Thermal-Hydraulic Codes for LWR LOCA and Transients. NEA/CSNI/R(96)17, July 1996.

[4] Proceedings ANS International Meeting on Best Estimate Methods in Nuclear Installations Safety Analysis (BE-2000); November 2000, Washington, DC, USA.

[5] BESSETTE, D.E. Initial and Boundary Conditions to LOCA Analysis — An Examination of the Requirements of Appendix K. Proceedings of ICONE 8, 8th International Conference on Nuclear Engineering, Baltimore, MD, USA; April 2-6, 2000.

[6] "Code of Federal Regulations, Title 10", National Archives and Records Administration, pp. 763-768; 1996.

[7] F. D'AURIA, M. LEONARDI, H. GLAESER, R. POCHARD: Current Status of Methodologies Evaluating the Uncertainty in the Prediction of Thermal-Hydraulic Phenomena in Nuclear Reactors; International Symposium on Two-Phase Flow Modelling and Experimentation", Rome, Italy, October 9-11, 1995.

[8] F. DEPISCH, G. SEEBERGER, S. BLANK: Application of Best-Estimate Methods to LOCA in a PWR; OECD/CSNI Seminar on Best Estimate Methods in Thermal-Hydraulic Safety Analysis, Ankara, Turkey, 29 June–1 July 1998.

[9] GLAESER, H.: Uncertainty Evaluation of Thermal-Hydraulic Code Results; International Meeting on "Best Estimate" Methods in Nuclear Installation Safety Analysis (BE 2000), Washington, DC, November 2000.

[10] M. LUDMANN, J.-Y. SAUVAGE: LB LOCA Analysis Using the Deterministic Realistic Methodology — Application to the 3-Loop Plant; 7th International Conference on Nuclear Engineering, Tokyo, Japan, 19-23 April 1999.

[11] CSNI Status Summary on Utilisation of Best-Estimate Methodology in Safety Analysis and Licensing; NEA/CSNI/R(96)19, October 1996.

[12] Proceedings of the OECD/CSNI Workshop on Transient Thermal-Hydraulic and Neutronic Codes Requirements, Annapolis, Maryland, USA, Nov. 5-8, 1996; NUREG/CP-0159, NEA/CSNI/R(97) 4, July 1997.

[13] Best Estimate Methods in Thermal Hydraulic Safety Analysis, Seminar Proceedings, Ankara, Turkey, 29 June–1 July 1998; NEA/CSNI/R(99)10, February 2000.
[14] Codes 2000, OECD-CSNI workshop on Advanced Thermal-Hydraulic and Neutronic Codes: Current and Future Applications, Barcelona, Spain, 12-13 April 2000.
[15] Validation Matrix for the Assessment of Thermal-Hydraulic Codes for VVER LOCA and Transients. A Report by the OECD Support Group on the VVER Thermal-Hydraulic Code Validation Matrix; NEA/CSNI/R(2001)4, April 2001.
[16] Regulatory Guide 1.157: Best Estimate Calculations of Emergency Core Cooling System Performance, U.S. Nuclear Regulatory Commission, May 1989.
[17] Nuclear Regulatory Commission, 10 CFR Part 50, Proposed Rule Making, October 30, 1998.
[18] VAN DOESBURG, W. et. Al, Fuel Safety Criteria Technical Review — Results of OECD/CSNI/PWG2 Task Force, Draft, 15 November 1999 (to be published).
[19] T. WICKETT et al, Report of the Uncertainty Methods Study for Advanced Best Estimate Thermal Hydraulic Code Applications, Volume 1 (Comparison) and Volume 2 (Report by the participating institutions). NEA/CSNI/R(97) 35, 1998.
[20] M.Y. YOUNG, S.M. BAJOREK, M.E. NISSLEY, L.E. HOCHREITER, Application of code scaling applicability and uncertainty methodology to the large break loss of coolant; Nuclear Engineering and Design 186 (1998) 39-52.

SAFETY MARGINS: DETERMINISTIC AND PROBABILISTIC VIEWS

J. HORTAL
Modeling and Simulation Area,
Consejo de Seguridad Nuclear (CSN),
Spain

Abstract. The meaning of the Term **"*Safety Margin*"** and other basic concepts used in safety analyses is sometimes ambiguous. There is a need to define a reference framework, where all these concepts could adequately be put in the right context. The Purpose of this paper is two-fold. On one hand, to derive a general concept of safety margin, where all the practical implementations of the concept could fit. On the other hand, to propose a unified view of current safety analysis methods, that allows, to identify how they complement each other or how they interact. Starting from basic definitions, some risk related concepts are derived to characterise the safety of a plant or the acceptable limits to be applied. Then, a global safety margin is defined and decomposed on several partial safety margins. Any safety analysis method should address the demonstration of these safety margins. This requirement is formulated through five steps that should always be followed. Current safety analysis method, that can be classified as deterministic and probabilistic, implement these concepts and steps in different ways. A comparison between both types of methods is done, pointing out their analogies and differences. An unified view based on the analogies and giving support for the differences is proposed as a way to deal with the principles of the so-called risk-informed regulation.

1. PURPOSE AND CONTEXT

The concept of safety margin is widely used in safety analysis. Sometimes, safety margins are defined and used in the context of a particular type of analyses where they have a precise meaning which is, however, difficult to export to other fields or speciality. In other cases, the qualitative use of the concept is apparently understood by everybody, but lack of consensus or even contradictions soon arise when going into the details. It should never be forgotten that the goal of the safety analysis is the design/assessment of the protection of a plant. This is a multidisciplinary task where inter-discipline communication is a need. For this purpose, it is essential to understand the global picture.

Since safety margins are very basic elements of the safety analysis, it should be possible to introduce, from very basic principles, a general concept of safety margin where all the practical implementations could fit. This is our purpose in this document. We have tried to derive the characteristics and elements of the safety analyses, including the concept of safety margins, from first principles. In addition, a comparative analysis between the so-called *deterministic* and *probabilistic* methods and how they implement the general concepts has been included.

In our understanding, and taking the American regulation[1] as a main reference, the topic is of particular importance when the risk-informed regulation is foreseen as an innovative philosophy for nuclear safety. The regulatory guidance of the NRC (see for example [1], [2]) includes five key principles to be met by risk-informed proposals and regulatory decisions. Three of these principles are the following:

1. The proposed change meets the current regulations unless it is explicitly related to a requested exemption or rule change.
2. The proposed change is consistent with the defense-in-depth philosophy.
3. The proposed change maintains sufficient safety margins.

[1]Nevertheless, the discussions and conclusions in this document can be extended to other regulatory systems.

It is also stated that risk analyses should be a complement, not a replacement of traditional analyses. However, there is no established method to achieve these objectives, especially when the impact of the change on the safety margins is not evident. In practice, this means that it is not easy to guarantee that current risk-informed methods are consistent with the principles and requirements of the current regulations, mostly based on the so-called deterministic analyses.

This document proposes a unified view of the *deterministic* and *probabilistic* approaches as a way to better understand the problem and to find ways of application of the regulatory requirements. The author wishes to acknowledge the valuable discussions and comments from other members of the Modeling and Simulation Area of the CSN: Enrique Meléndez, José M. Izquierdo, and Miguel Sánchez.

2 SOME DEFINITIONS[2]

- A **facility** or a **plant** is a set of interrelated systems with a common objective.

- A **system** is a set of components, articulated in a certain way, that performs a system function as a part-task of the facility function.

- The systems of a facility are primarily designed to obtain a benefit by performing several operating functions. However, the operation of the facility may involve some risk, i.e. there is some chance that an undesired effect be produced. Because of that, some systems or some system features are designed to prevent or mitigate those undesired effects. These are called **protections** of the facility.

The state of the facility is described by:

- The **logical state**[3], *j*, is a set of integer (discrete) variables describing the states of facility systems and/or components (nominal, derated, failed in a given mode, etc).

$$\mathrm{j} = \{\mathrm{j}_1, \mathrm{j}_2, ..., \mathrm{j}_N\} \tag{1}$$

where *N* is the number of systems/components of interest.

- The process vector, $\vec{x}$, is a set of real variables describing the facility process evolutions (temperatures, flows, etc.).

Given a logical state *j* and a set of initial conditions of the process variables, denoted by x_o, the evolution of the process vector is described by functions of the form:

$$\vec{x}_o = \vec{g}_j(t, x_o) \tag{2}$$

where *t* represents time. The vector $\vec{g}_j$ is called **facility dynamics for logical state *j*.**

An **event**, represented by E^t is an instantaneous change in the plant logical state *j*, occurring at time *t*. Note that, in the general case, an event will change the plant dynamics.

Assuming that the plant is in a steady state, i.e. a time independent state of both *j* and $\vec{x}$, an event E^0 (called **initiating event** or **initiator**) may trigger a transition in the plant

[2]Most definitions are taken from reference [4]

[3]It is sometimes called status vector.

dynamics which makes the process vector to be no longer steady. New events may occur afterwards as a consequence of the process vector evolution or due to some stochastic process or by a combination of both. The evolution continues until a new steady state is reached. All the history between the initial and final steady states is generically referred to as a **transient**.

It was already mentioned that the facility may generate undesired effects, i.e, damages. In some cases, damages can be catastrophic, including the destruction of the plant itself or severe damage to the environment, personal health or properties. A **damage variable**, is a function $D_i(\vec{x},t)$ of the process vector that quantifies the generation of an undesired effect (damage) or the proximity to that effect.

Different operating situations, from normal operation to destructive transients, generate different amount of damage but, fortunately, they are not equally frequent. The risk of a facility is an attribute of the relationship between amount of damage and likelihood of this damage to occur. The usual measure of likelihood in risk studies is frequency.

In some cases, the term "risk" is used to quantify the mean frequency of a particular range of values of a single damage variable. This could provide a numerical value of the "risk" but it is only a partial measurement of the risk. Any attempt to formalize the risk concept cannot rely on such a restrictive definition.

Even in the case of considering a single damage variable, it is not possible to quantify the risk with a single numerical value, since the concept is essentially bidimensional. A given amount of damage can be unacceptable if it occurs very often, but the same damage can be acceptable if it is very unlikely to occur. The acceptability threshold will be, of course, different for different amounts of damage.

When several damage variables are considered, which is the usual case, different risk analyses must be performed for each damage variable. The complementary term of risk is safety. A plant is **safe** if no unacceptable damage is expected from its operation, i.e. if no unacceptable results have been found with respect to any damage variable.

It has been already mentioned that the acceptability of an amount of damage is a function of its expected frequency. Given a damage variable, D_i, the **damage limit** is a function that defines, for each value of frequency ν, the maximum acceptable damage:

$$D_i^L = D_i^L(\nu) \tag{3}$$

Also the inverse function can be used which gives, for each value of D_i, the maximum acceptable frequency ν^L:

$$\nu^L = \nu^L(D_i) = (D_i^L)^{-1}(D_i) \tag{4}$$

Let us consider the **risk plane** associated to damage variable D_i, whose coordinates are the damage magnitude as abscissa and the frequency (usually in logarithmic scale) as ordinate. The damage limit can be represented as a curve in this plane. In the following section we are discussing some properties of the damage limits and its graphical representation.

3. CHARACTERIZATION OF THE DAMAGE LIMIT

Every damage limit should be established with criteria based on public health, environment protection, property integrity, including the integrity of the plant itself, etc. Therefore they are subject to social and political considerations. However, they should meet also some technical criteria that we are going to analyze. Generally speaking, we could say that the technical criteria allow to characterize the shape of the damage limit curve while other criteria define the exact position of the curve in the risk plane.

The first obvious characteristic of the damage limit is that it must be a monotonic decreasing function. The higher the frequency, the lower the allowed damage.

The normal operation of the plant include situations from frequent events to steady state, i.e. frequencies ranging from high to infinity. The value of the damage variables in normal operation should be acceptable because, otherwise, the plant could not operate. In other words, there should be a minimum value of the damage below which the frequency is not limited. This means that in the low damage, high frequency region of the risk plane, the damage limit tends to be vertical.

For some damage variables, there is a threshold value below which no real damage is generated. In this case, lower values of the variable may be used to indicate the level of proximity to the damage condition. Normal operation values must be, of course, below the threshold. Consider, for example, the damage derived from the melting of a particular structure; the damage variable could be the maximum local temperature in the structure and the threshold would be the melting point of the material.

In other cases, any non-null value of the damage variable indicates real damage. In these cases, some level of damage will be generated during normal operation, but it must be maintained below acceptable limits. This is the case, for example, of the flow of polluting effluents from an industrial process.

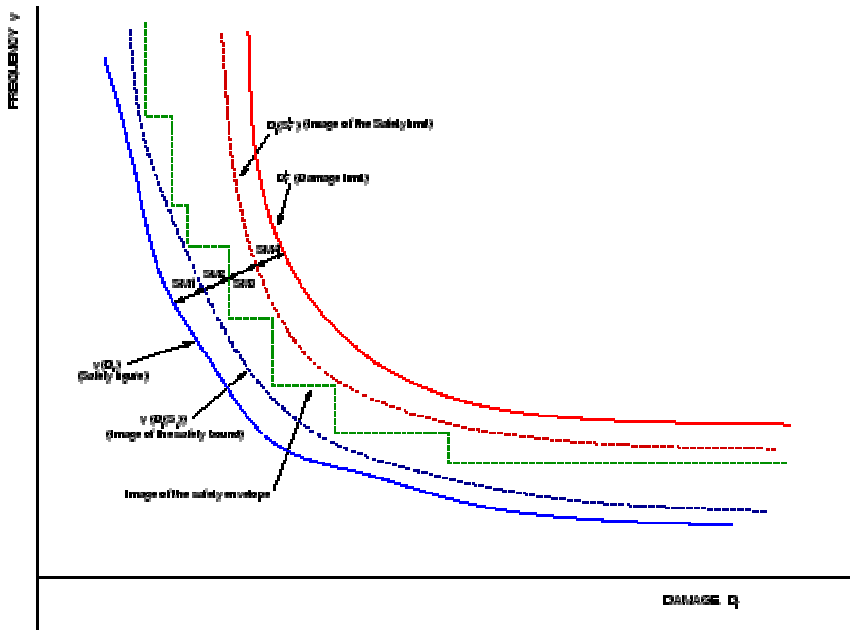


Figure 1: Qualitative representation of safety concepts in the risk plane.

High values of damage are prevented by a well designed set of protections. However, there could be situations not covered by the protection design, for instance, situations where the protection fails. High damages, even catastrophic, can be generated in these situations. A better design of the protections or an improvement of emergency procedures (that can be considered as non-automatic protections) will make these situations more and more unlikely. However, the eventuality of a catastrophic damage cannot be totally eliminated. Since the design of protections cannot be extended to infinity, it is necessary to consider a frequency threshold, representing the credibility limit. A frequency below this limit means that the situation is so unlikely that can be ignored. In other words, for frequencies below the credibility limit the amount of damage is not limited. As frequency decreases towards the credibility limit, the damage limit increases to infinity. This means that, in the high damage, low frequency region, the curve of the damage limit tends to be horizontal.

With the conditions imposed so far, i.e.

- Monotonically decreasing function.
- Vertical limit or asymptote on a low damage value.
- Horizontal limit or asymptote on a low frequency value

the general shape of the damage limit will be like the one represented in Figure 1

4. CHARACTERIZATION OF THE PLANT SAFETY

The plant safety (or plant risk for pessimistic people) evaluation consists, in theory, on the determination of the expected frequency of occurrence of each damage amount[4]. Damage is generated as a consequence of the plant behavior during normal operation or due to possibly non-programmed transients.

A transient (including normal operations as particular cases), represented by the symbol q can be viewed as a composite event given by a combination of an initiating event (or initiator), E_0, occurring at t_0 from stationary initial conditions $\underset{\sim}{x}_0, j_0$, and subsequent events occurring at some time points (**transition times**) after the initiator, i.e.

$$q = \{E_0^{t_0}, E_1^{(t_1-t_0)}, E_2^{(t_2-t_0)}, ..., E_N^{(t_N-t_0)}$$

Also, a transient can be viewed as a dynamic history of the process vector that depends on the initial conditions and the logical state evolution:

$$\underset{\sim}{x}(t) = G_q(j(t, \underset{\sim}{x}), \underset{\sim}{x}_o) \tag{5}$$

where G_q represents the concatenation of all the dynamics $\underset{\sim}{g}_j$ that participate in the transient.

Two transients would be strictly identical if the same initiating event occurs from the same initial conditions and the same subsequent events occur at the same transition times. The resulting evolutions of the process vector for two identical transients would also be identical. However, since the space of initial conditions (given by the stationary values of the process vector $\underset{\sim}{x}$ for the logical state j_o) and the transition times are, in general, continuous random variables, two transients will never be strictly identical and the concept of frequency of a transient does not make sense.

[4]It should be recalled that this evaluation must be done for every damage variable.

Let us discretize the space of the initial conditions by partitioning the space of $\vec{x}$ into a number of ranges and considering that two stationary values of $\vec{x}$ are identical if they belong to the same range. Similarly, we can discretize transition times and consider that all the times belonging to the same range are identical. Two transients may then fullfill the conditions to be considered identical. The discretization or partition is only valid if the dynamic histories of two identical transients are identical, i.e. if there is a small ε such that, for any t, $|\vec{x}_1(t) - \vec{x}_2(t)| \le \varepsilon$. From now on, we will use the term *transient* referring to a class or group of identical transients and two identical transients will be considered as two occurrences of the same transient.

With these premises, each transient q can be considered as a random process, characterized by its mean frequency ν_q, and producing a dynamic history $\vec{x}(t)$ whose main characteristic from the safety point of view is the history of the selected damage variables $D_{iq}(G_q, t)$.

A damage of magnitude D_i occurs whenever a transient q generating a damage $D_{iq} \ge D_i$ occurs. Therefore, the frequency of a given amount of damage is given by:

$$\nu(D_i) = (q|D_{iq} D_i)\nu_q \qquad (6)$$

Equation (6) defines a figure of merit of the plant safety since it gives the expected frequency of each damage value. This function can be represented as a staircase-shaped curve in the risk plane but, as the discretization of the initial conditions and transition times is made finer, the staircase tends to be a continuous curve. The limit curve, that we define as the **safety graph** of the plant, has been represented in the risk plane of damage variable D_i (see Figure 1) along with the damage limit(4). If the curves do not cross each other, i.e. if, $\nu(D_i) \le \nu^L(D_i)$ for every value of D_i, the plant can be considered safe.
There are *only* two drawbacks to this approach:

- Most damage variables are difficult to measure in the plant and cannot be used to trigger protections. This makes them unpractical for safety evaluation.
- The limit curve of function (6) cannot be calculated due to the unlimited number of transients to be considered.

5. SAFETY VARIABLES AND SAFETY LIMITS

Damage variables are easy to define; they can be more or less easy to calculate and, in many cases, they are difficult to obtain from the process variables measured in the plant. When this occurs, the protection design relies on other variables related with the damage conditions. A typical case is that the damage variable depends on phenomena that are both difficult to monitor and difficult to simulate. The detection of the proximity to the damage condition should then be based on other variables more easily related with measured process variables. These variables are called **safety variables** $S_i(\vec{x}, t)$. In general, they are different from the damage variables, but we can assume that for every damage variable D_i there is an associated safety variable S_i.

An important part of the protection design is the selection of the safety variables. They are, like the damage variables, functions of the process vector. Also, they are subject to limits that depend on frequency in order to prevent unacceptable damage. In the practical implementation of the protection, safety variables are a replacement of the damage variables.

However, there is an important difference. Since they do not detect damage (unless they are also damage variables), the limits are not established in terms of acceptable damage. The limits imposed to safety variables represent, instead, **necessary conditions for damage**.

Given a damage variable D_i, a safety variable S_i can be associated to it if there is a function $D_I(S_i)$ such that

$$D_I(S_i(\vec{x},t)) \geq D_i(\vec{x},t) \tag{7}$$

at least for conditions of $\vec{x}$ that make D_i be close to the limit D_i^L. The bounding condition (7) is usually demonstrated through generic one-time studies that may involve considerable complexity and eventually be based on specific experiments. Sometimes, the condition (7) is actually composed of a chain of two or more bounding conditions of the same type with intervention of intermediate variables. In such case, any intermediate variable can also be considered as a safety variable.

Once the safety variable has been selected, the damage limit can be replaced by a safety limit

$$S_i^L = S_i^L(\nu) \tag{8}$$

such that

$$D_I(S_i^L(\nu)) \leq D_i^L(\nu) \tag{9}$$

for every ν.

The safety limit can also be represented as a limiting frequency given by the inverse function of(8)

$$\nu^L = \nu^L(S_i) = (S_i^L)^{-1}(S_i) \tag{10}$$

as in the case of the damage limit.

The function on the left-hand side of (9)is the image of the safety limit on the risk plane of the damage variable D_i. It has been represented in Figure 1.

A figure of merit similar to (6)can be defined if safety variables are used in the place of damage variables. If S_{iq} represents the worst value of S_i along a transient q, the frequency of each value of the safety variable can be calculated as

$$\nu(S_i) = \sum_{(q|S_{iq}\,\phi\,S_i)} \nu_q \tag{11}$$

Where the symbol ϕ, meaning “equal to or worse than”, has been used instead of $\geq$ since there are cases where lower values of S_i may be indicative of higher damage. The function (11) will be referred to as **safety bound** because, due to condition (7), the image of this function on the risk plane of D_i, given by $\nu(D_I(S_i))$, is an upper-bound approximation to the safety graph. It has been represented also in Figure 1.

If the safety bound (11) does not cross the safety limit, i.e. if $\nu(S_i) \le \nu^L(S_i)$ for every S_i, the plant safety is guaranteed. A violation of the safety limit, however, does not mean necessarily a violation of the damage limit, due to the inequalities in expressions (7) and (9). Unfortunately, as in the case of damage variables, expression (11) cannot be calculated because of the unlimited number of terms in the summation.

6. GROUPING AND ENVELOPING TRANSIENTS

The practical approach to deal with an unlimited number of transients is to group them. Instead of considering each individual transient, we consider a finite number of groups of transients having common characteristics whose nature is not important to define now. A group of transients, denoted by Q, can be characterized by its collective frequency

$$\nu_Q = \sum_{q \in Q} \nu_q \tag{12}$$

and by a bound D_{iQ} of the damage generated by the grouped transients, i.e.

$$D_{iQ} \ge D_{iq} \qquad \forall q \in Q \tag{13}$$

In terms of the associated safety variable, the group can also be characterized by the bounding value S_{iQ} of this variable,

$$S_{iQ} \; \phi \; S_{iq} \qquad \forall q \in Q \tag{14}$$

If any possible transient is included in some group, i.e. if the grouping is complete and we apply all the concepts related to safety evaluation to these groups, the expressions (6) and (11) become, respectively,

$$\nu(D_i) \le \sum_{(Q|D_{iQ} \ge D_i)} \nu_Q \tag{15}$$

$$\nu(S_i) \le \sum_{(Q|S_{iQ} \phi S_i)} \nu_Q \tag{16}$$

The right-hand sides of the expressions (15) and (16) are step-wise functions in the respective risk planes of D_i and S_i. These functions are envelopes of the theoretical functions (6) and (11), respectively, as denoted by the inequalities, both in (15) and (16) and in (13) and (14)

The safety analysis can now be redefined in terms of safety variables. The function (16), that we call **safety envelope** of the plant, may be used as the practical figure of merit of the plant safety. The image of the safety envelope on the risk plane of D_i has also been represented in Figure 1. If the safety envelope does not cross the safety limit (10), the theoretical functions (6) and (4) can be guaranteed not to cross it either. In Figure 1 this condition, along with the definition of the safety envelope, means that the step-wise image of the safety envelope cannot cross either of the images of the safety limit and the safety bound. Therefore, the following is a sufficient condition for a plant to be considered safe:

$$\sum_{(Q|S_{iQ} \phi S_i)} \nu_Q \le \nu^L(S_i) \qquad \forall S_i \tag{17}$$

This expression has the advantage that there are methods for estimating both ν_Q and S_{iQ} and, therefore, it represents a practical solution of the safety assessment problem. Nevertheless, the estimation of ν_Q and S_{iQ} is far from being trivial and, in many cases, only approximated solutions are possible. In consequence, the safety assessment is, still, a very difficult problem.

Note that the selection of the parameters that characterize a group of transients (12), (13) and (14) is not arbitrary. Alternative selections do not allow, in general, to conclude that the fulfillment of the condition (17) guarantees the safety of the plant. In particular, S_{iQ} cannot be defined as an average of the form

$$S_{iQ} = \frac{\sum S_{iq} \nu_q}{\sum \nu_q}$$

and the frequency of the group cannot be defined as that of the most frequent transient in the group.

Once a complete grouping of transients has been defined, each group can be replaced by a single transient, no matter realistic or artificial, that generates a damage greater than or equal to the characteristic damage of the group and with an assigned frequency equal to or greater than the frequency of the group. These new transients can be, again, regrouped using the same criteria of previous groupings and a new sufficient safety condition similar to (17) will result from the process.

7. THE CONCEPT OF SAFETY MARGINS

Several of the mathematical expressions used so far involve inequalities. Whenever a comparison is done, or an envelope is defined, an inequality appears. And whenever an inequality appears, a margin can be defined. The overall safety margin would be the distance between the safety graph (6) and the damage limit (3). This distance is not a number but a function and can be defined in several ways, for instance, difference in damage for a given frequency, difference in frequency for a given damage or a combination of both. Whatever the definition, the safety analysis should be oriented to demonstrate that the safety margin exists and to identify the circumstances that make it increase or decrease.

From the above discussion it is clear that the introduction of concepts like the safety variables or methods like transient grouping and bounding, allows one to decompose the safety margin into partial safety margins.

The selection of a safety variable S_i associated to D_i introduces in the risk plane of D_i the image of the safety bound. The distance between this curve and the safety graph is the first partial safety margin (SM1). The definition of the safety limit S_i^L determines its image in the risk plane of D_i and the distance between this image and the damage limit is another partial safety margin (SM4).

In addition, the grouping and enveloping process described in section introduces two more partial safety margins given by the respective distances between the safety bound and the safety envelope (SM2) and between the safety envelope and the safety limit (SM3) (or between their respective images in the plane of D_i).

The partial safety margins SM1 to SM4 have been represented in Figure 1, where the double ended arrows do not represent any particular definition of distance between curves. They must be interpreted only as a qualitative illustration of the concept.

Summarizing all the above discussions, a complete safety analysis would consist in the following (big) steps:

- Determination of the damage variable D_i and the damage limit D_i^L.
- Determination of the safety variable S_i (and the corresponding function D_I). Demonstration of the existence of the partial safety margin SM1.
- Determination of the safety limit S_i^L. Demonstration of the existence of the partial safety margin SM4.
- Determination of the safety envelope as a result of grouping and enveloping of transients. Demonstration of the completeness of the grouping and demonstration of the existence of the partial margin SM2.
- Demonstration of the existence of the partial margin SM3.

These steps must be repeated for every damage variable of interest. Note that the partial safety margins must be demonstrated, not necessarily calculated. If no partial safety margin results negative, the plant safety will be guaranteed.

8. PRACTICAL APPROACHES TO SAFETY ANALYSIS

The practical implementation of safety analysis principles has resulted in two main types of methods. They are known as *deterministic* and *probabilistic* methods, although these denominations can be a little bit misleading as we will comment later. In this section, we are trying to describe the most salient characteristics of each type and to show how they fit into the scheme delineated in the previous sections.

8.1. What is the deterministic analysis?

In the so-called *deterministic* methodology whose results (in the American regulatory model) are summarized in the chapter 15 of the Final Safety Analysis Report (FSAR), a set of design basis events (DBE) which trigger challenging transients are selected and grouped in different frequency classes (called *Conditions*). Following the classification of ANSI-51.1/ANSI-N18.2, [3] normal operation maneuvers are classified as *Condition I*. The *Condition II* groups events such that any of them may occur during a calendar year. *Condition III* includes events any of which may occur during the plant life. Finally, *Condition IV* events are very unlikely events that, due to the potential severity of their consequences, give rise to specifically designed automatic protections. This classification clearly shows that even in the chapter 15 analysis (very often considered as the paradigm of the *deterministic* analyses) there are some *probabilistic* elements.

The design basis events (DBE) (and the subsequent design basis transients (DBT)) take their name from the fact that they are used to **design** the automatic protections. A **necessary** condition for a plant to be safe is that, for any anticipated or postulated event, there is at least a protective function able to prevent unacceptable damage. Starting from this statement we can analyze three aspects:

1. **What is unacceptable damage?** This can be a subject of discussion, but in the *deterministic* analyses there are explicit criteria. For example, in the case of the ANSI-51.1/ANSI-N18.2, some of the requirements, related to the fuel integrity for each *Condition*, are the following: no fuel clad damage is allowed for *Condition I* and *II* events; for *Condition III*, a number of damaged fuel pins is allowed, but not an extensive core damage; finally, for *Condition IV* events there is no limit in the number of damaged pins, but the core geometry must remain unchanged to keep it coolable. These criteria, that represent a step-wise damage limit, are usually redefined by the designers in terms of safety variables like DNBR values or cladding temperatures.

2. **How can it be assured that the unacceptable damage is prevented?** One of the criteria used to select the DBEs is that they must provide a bounding value of the amount of damage[5] (whatever be the damage definition) generated during the transient. This way, it is assured that, if no DBT overpasses the limit of the unacceptable damage, there will be no real transient that overpasses that limit. From these considerations there is a clear need to calculate with some accuracy the damage associated to the design basis transients.

3. **Is there a protective function for every transient?** Or, in other words, how could we find a set of design basis transients that are a complete envelope of all possible transients included in the design basis scope? The answer to this question leads to each designer's own methodology which is highly sophisticated and subject to very strict proprietary restrictions.

Assuming that the previous condition is met, the plant can only be safe if **every time** that a protection is called for intervention it **actually works** on time. We can identify here a second *probabilistic* element in the *deterministic* analysis. It is implicitly assumed that the failure probability of the protection is **very low** and the way to implement this assumption is the **single failure criterion**. Every protective function must accommodate any single failure (in addition to the initiating event) without loosing its functionality and the eventuality of more than one failure is considered very unlikely.

Note that in the above considerations there is not a word about the conservatism or the realism of the simulation models. It is clear that the use of more conservative models or assumptions for the calculation of the damage envelope will add some extra margin between the envelope and the "real world" (i.e. between the safety envelope and the safety graph). But it is also clear that the calculated damage will not be a bound unless the models and assumptions used to simulate the design basis transient reflect **at least** the worst case of the class that the transient represents.

In summary, the important characteristics of the *deterministic* analysis that we want to stress here are the following:

- Any (initiating) event can be classified in a *Condition* or frequency group , or in a residual group of "beyond design basis events".

[5]The term "amount of damage" or simply "damage" includes also the proximity to the damage condition for those transients that produce no real damage.

[6] Note that the frequency of the event does not determine its classification. The events are grouped by other criteria like demanded protections or expected damage. The frequency of the resulting group determines the Condition where all the grouped events are classified.

- The *probabilistic* elements of the analysis are addressed by implicit or explicit assumptions but no probability calculation is performed.

- From the point of view of the subsequent evolution, any event in the design basis region can be classified in a class whose representative is a design basis event.

- A design basis transient usually consists of an initiating event (design basis event) that triggers a single protective function able to terminate the transient while preventing unacceptable damage.

- The damage associated to a design basis transient must be a bound of the damage of any transient included in its class. This bounding damage (or its corresponding bounding value of the safety variable) is calculated with more or less detailed simulation models.

- The concept of unacceptable damage can be precisely defined for each frequency class.

The *deterministic* analysis implements the five steps enumerated in section 0 in the following way:

- **Determination of the damage variables and the damage limits**. The limits imposed by ANSI-51.1/ANSI-N18.2 or any equivalent standard clearly determine the damage variables and their acceptability limits. Usually, the damage limit is defined as a step-wise function by imposing different limiting values for different frequency ranges. The transient grouping process is made in a way such that the estimated collective frequency of the transients classified in a *Condition* falls into the range of the corresponding step of the damage limit. In addition, the collective frequency of the transients not included in any condition (i.e. classified as *beyond design basis*), is lower than the lower frequency of the highest *Condition*. The result is that the safety envelope "staircase" has the same number of steps than the damage limit (see Figure 1) and, therefore, the safety margins, measured in damage or safety variable units, are *Condition* specific. No damage limit is defined for "beyond design basis" events.

- **Determination of the safety variables. Demonstration of the existence of the partial safety margin SM1**. It was mentioned above in this section that the damage limits are usually redefined by designers in terms of safety variables. An illustrative example is the use of the DNBR as a safety variable in PWR-Westinghouse plants. Experiments and theoretical studies show that there is a relationship between local DNBR values and thermomechanical stress in the fuel cladding. It is, therefore, possible to correlate the minimum DNBR value in the core with likelyhood of fuel cladding damage and, consequently, with the maximum expected number of damaged pins. This correlation introduces a safety margin SM1 in the analysis.

- **Determination of the safety limits. Demonstration of the existence of the partial safety margin SM4**. This step is actually parallel to step 2. The same correlations that allow the replacement of damage variables by safety variables allow, at the same time, the replacemet of the damage limit by a safety limit. Continuing with the example of the DNBR, the safety limit applicable for *Condition I* and *Condition II* transients is a particular value of the DNBR. Traditionally, this limit was fixed at DNBR = 1.3 based on the W3 correlation. Nowadays, more accurate methods allow for lower values that incorporate both generic and plant-specific contributions, including uncertainties in plant instrumentation. This limit assures with a 95% confidence that, with a 95% probability, no

fuel pin is expected to be damaged and therefore, assures the existence of the safety margin SM4. This limit is the one to be checked by the analysis. However, since DNBR is not a process variable, it is necessary to correlate it with process variables in order to trigger the protective actions. There is a particular combination of process variables[7] such that, if maintained lower than a limit (that depends also on some process variables) assures that the minimum DNBR in the core is maintained above 1.3. The term "safety limit" is often applied to the limiting value of such combination of process variables.

- **Determination of the safety envelope as a result of grouping and enveloping of transients. Demonstration of the completeness of the grouping and demonstration of the existence of the partial margin SM2**. There is a double grouping of transients in the *deterministic* analysis. The classification in *Conditions* has been extensively commented. Also, it has been mentioned that, in each *Condition*, a number of design basis transients are selected with the aim of determining an upper bound of damage. This means that the transients grouped in a *Condition* are sub-classified into smaller groups, each of them represented by a design basis transient. The analysis must demonstrate that any transient is represented by a design basis transient unless it is classified as "beyond design basis". The correct selection of the design basis transients assures the existence of the safety margin SM2. The sub-classification has the only objective of finding the safety envelope segment for the *Condition* and in no case the frequency of each subgroup is taken into consideration. It is important to point out that the sub-grouping and the selection of the design basis transients may be different for different damage or safety variables.

- **Demonstration of the existence of the partial margin SM3**. The comparison of the safety envelope, given by the results of the design basis transients, and the safety limit, allows to check the existence of the safety margin SM3 and, therefore, to conclude the analysis.

8.2. What is the probabilistic analysis?

The design of automatic protections is a very practical problem with very complex solutions. Because of that, the automatic protections cannot be designed to cope with any possible situation since this would lead to an endless design process [5]. Real life, therefore, does not always fit into design assumptions and some plant transients may go beyond the design basis envelope, i.e. they cannot be represented by any design basis transient. There are a number of reasons that could lead to this situation, among possibly others:

- The initiating event occurs from initial conditions not considered in the selection of the design basis events.
- There are concurrent "initiating" events, either simultaneous or subsequent.
- There are more than one failure additional to the initiating event, and the protective function does not work or fails to arrest the transient.
- Human intervention takes the evolution of the transient away from the design conditions.

The question is then, what if such situations occur?

The *probabilistic* analysis[8] was developed to deal with these situations. It does not take for granted the actuation of the protective functions. Instead, the protections are assumed to fail with some probability. There are three main aspects of the problem:

[7] This combination is used in the overtemperature ΔT protection in Westinghouse plants.

[8] The following comments assume the identification of *probabilistic* analysis with Level 1 PSA. The extension of these arguments to level 2 is possible but it has not been done here for simplicity.

1. **What are the possible evolutions of the situation?** This question is addressed by considering that, once a protective function has failed, some other protection will be called either automatically or manually. The new function could, again, be effective or fail, and the process continues recurrently. The number of possible combinations of initial conditions, initiating events, protective functions failures and successes and times of protection intervention is virtually infinity. It is then necessary to select some families of transients that represent all the possibilities. In the *probabilistic* analysis, a **sequence** may be defined as a group of transients having the same combination of initial conditions, initiating event and protection interventions or failures. The term *sequence* is also often used to refer to a particular transient which is considered as a representative of a sequence. All the sequences originated from the same initiating event with the same initial conditions form a family which is known as *event tree*. The protections that could eventually be demanded are represented as "headers" of the event tree. Some considerations about the criteria that should be used to select the set of representative event trees are given below.

2. **How often could they occur?** The question can be divided in two parts:

    - How often can we expect a situation requiring the intervention of some protection? or, in other words, how often can we expect an initiating event?
    - What is the probability of effective intervention of each demanded protection?

The answer to these two sub-questions allows one to evaluate the expected frequency of each possible sequence identified from question 1. The probability of the protection failure is calculated from a logical structure, called *fault tree* that relates the failure with the occurrence of some basic events. Both the initiating event frequency and the basic event probabilities are estimated by several means including historical data, laboratory tests, experience from other industries, etc.

3. **How much damage can be expected from each evolution?** The *probabilistic* analysis does not try to find a very accurate answer. The only thing that matters in this context is whether the core damage will be severe. If not, the evolution is considered "successful". This simplification makes sense only when the **existence** of the *deterministic* analysis is taken into account, because that analysis already deals with non-catastrophic damages. For this reason, the focus of the *probabilistic* analysis is put on the identification of sequences leading to severe core damage and the expected frequency of that damage.

Going back to the selection of representative event trees, it is clear that the initiating events (including in its definition the initial conditions from which they occur) used in the analysis must be representatives of groups of possible real initiating events. The frequency assigned to the initiating event is the collective frequency of all the events included in the group. The selection of the representative event should guarantee the safety margins. Therefore, as a general criterion, the representative should be an initiating event that produces the worst results, although the meaning of "worst" can be very hard to delimit.

Also, each individual sequence of the tree represents groups of transients with the same combination of successes/failures of the protections (i.e. the same header states) but with differences in timing or even in the order of the events. Not all the combinations are considered in the event tree. Some criteria as for example logical elimination or frequency

truncation lead to the reduction of the number of sequences in the tree. Also, some rules can be applied to conservatively group sequences with different header states.

In summary, the important characteristics of the *probabilistic* analysis that we want to stress here, are the following:

- Any sequence included in the analysis is classified from the damage point of view as "success" or "core damage".
- In general, damage is not calculated. Instead, its estimation is derived from the header combination in the sequence. Supporting or confirmatory calculations are sometimes performed but in most cases they are not a cornerstone of the method.
- Any possible plant transient should be covered by the set of sequences of the *probabilistic* analysis. However, the identification of a transient with a single sequence will, in general, be difficult to do. A frequent case is that different parts of the transient are represented by different parts of sequences in the analysis.
- An event tree consists of an initiating event, defined from given initial conditions, and all the realistically possible combinations of success/failure of the involved protective functions.
- The frequency of each sequence in the tree is calculated from the frequency of the initiator, detailed logical models of protection failures and basic probability data. Since each sequence is actually a representative of a group, its frequency should be at least equal to the collective frequency of the transients included in the group.
- It would be possible to define an "acceptable core damage frequency limit". However, the lack of homogeneity among the *probabilistic* models used by different analysts in different plants does not allow to implement this concept. Instead, the core damage frequency (CDF) obtained for each plant by the PSA analysis is taken as a reference value for later reevaluations.

The level-1 PSA, as a prototype of *probabilistic* analysis, implements the five steps enumerated in section 0 in the following way:

- **Determination of the damage variable and the damage limit**. The only damage variable is the loss of core geometry due to high temperature. Since the objective of the analysis is to obtain a frequency value, it is more convenient to use in this case the frequency limit given by the inverse function of the damage limit (expression 4). However, it has been already said that such limit has not been defined so far.
- **Determination of the safety variable. Demonstration of the existence of the partial safety margin SM1**. Core (cladding) temperature can be used as safety variable to detect the proximity to the loss of core integrity. Other variables are often used to detect situations that are assumed to inevitably evolve towards the damage condition, such as loss of cooling sources. However, it has been mentioned that the damage condition is not explicitly calculated in most cases and, consequently, the safety variables are not necessarily well identified in the analysis. Therefore, the existence of the margin SM1 is demonstrated only qualitatively in many cases.
- **Determination of the safety limit. Demonstration of the existence of the partial safety margin SM4**. Since the frequency limit for core damage is not defined, it makes no sense to define a safety limit or a frequency limit for safety variables. Therefore, the safety margin SM4 is not taken into consideration.

- **Determination of the safety envelope as a result of grouping and enveloping of transients. Demonstration of the completeness of the grouping and demonstration of the existence of the partial margin SM2**. The safety envelope in the *probabilistic* analysis is the value of the core damage frequency obtained from the set of event trees included in the analysis. This frequency is the collective frequency of all the sequences leading to core damage. Taking into account the definition of sequence given above, it is clear that the delineation of the sequences is the practical implementation of the grouping process. The delineation methods are carefull in the determination of all the possible (credible) combinations of headers in order to assure the completeness of the grouping. Each sequence is characterized by a frequency and classified as *damage* or *success*[9]. According to sections 0 and 0, the partial safety margin SM2 exists if the sequence frequency is actually greater than or equal to the collective frequency of all the transients grouped in the sequence and if no transient leading to core damage is represented by a sequence classified as success. These two conditions are not explicitly addressed in the analysis, but the methods are assumed to guarantee its fulfillment.

- **Demonstration of the existence of the partial margin SM3**. Since no safety limit has been defined, the partial safety margin SM3 is not taken into account.

9. A UNIFIED VIEW OF THE SAFETY ANALYSIS

From the previous section it is clear that there are many analogies and some differences between the *deterministic* and the *probabilistic* approaches. In this section we try to show that they are actually the two faces of the same coin.

The main analogy from which all the other analogies are derived is the similarity between event trees and design basis transients. Both are representations of the evolution that follows an initiating event, and in both cases a frequency is assigned to the initiating event. Moreover, both of them are enveloping representatives of groups of evolutions with common characteristics. A design basis transient can be viewed as a particular case of event tree with a single header whose corresponding failure branch has been truncated by low frequency[10]. As a result, the frequency of the only sequence resulting from a design basis event (i.e. the frequency of the design basis transient) is equal to the frequency of that event, while in the general case the frequency of a sequence is the product of the initiating event frequency and the probability of the header combination. Also, the design basis transients can be viewed as particular sequences in a complete set of event trees.

The differences are mainly related with the assumptions of the protection actuation and with the primary objective of the analysis:

- In a design basis transient the actuation of the protection is assumed because the focus is on the higher frequency ranges. Protection failures are expected to be of low probability and they are considered only in the *probabilistic* analysis that focuses on low frequencies.

---

[9] All the sequences that have been elliminated by low frequency form a residual group of non-credible sequences whose collective frequency is small with respect to the resulting core damage frequency. Taking this group into consideration, the grouping process can be considered complete.

[10] Some assumptions of some DBTs are equivalent to consider other headers in predefined states with probability 1. These assumptions can also be interpreted as boundary conditions of the initiating event that magnify the challenge to the protective function associated to the DBT.

- The evaluation of a design basis transient is the determination of an amount of damage while the evaluation of an event tree consists of the determination of a frequency, namely, its contribution to the core damage frequency.

A common argument used when comparing *probabilistic* and *deterministic* analysis methods is that the former are more realistic while the latter are too conservative. In our opinion this is a false controversy because of the following reasons:

- Both methods are based on the use of envelopes, and this is an intrinsic characteristic of any safety analysis, as shown in sections 0 to 0. The degree of conservatism contained in the models and assumptions of the analyses results in a different "distance" between *reality* and *envelope*, i.e. different size of the safety margins. Both methods try to reduce unneeded conservatism but in any case the enveloping character of the analysis must be guaranteed.

- Concerning frequency **calculations**, the *probabilistic* analyses are much more detailed, but the methods to obtain input data are, still, plenty of bounding assumptions. They are, perhaps, more realistic than the **estimation** of frequencies made in the *deterministic* case, but it should be recalled that the objective is to find an envelope rather than to describe the reality.

- With respect to damage calculations, the situation is the opposite. *Deterministic* analyses are much more detailed and, despite the use of more or less conservative models and assumptions, a **calculated** result is likely more realistic than an **estimation** based on the pure combination of event tree headers. However, the objective, again, is not realism but safety.

In summary, both methods apply its main power in the aspect they focus: damage in the *deterministic* case and frequency in the *probabilistic* one. In its respective field, each method is more detailed and likely more realistic, but in the other's field both of them use rough approximations.

There can be lots of reasons for the differences in focus and accuracy between both types of analysis. However, just from the above discussions, it can be seen that these differences make sense.

Let us consider a single risk plane where the damage variable is an abstraction of all the damage variables representing a particular gradation of all the possible damages (Figure 2). Let us also assume that a damage limit can be defined for this damage variable, like the one represented by the solid curve in Figure 2 or like the more practical step-wise definition given by the dashed line in the same figure.

Let us also assume that a complete partition of the transient space has been done with the aid of a set of event trees, resulting in a set of sequences that include, as particular cases, the design basis transients. These sequences can be ordered by the damage they generate.

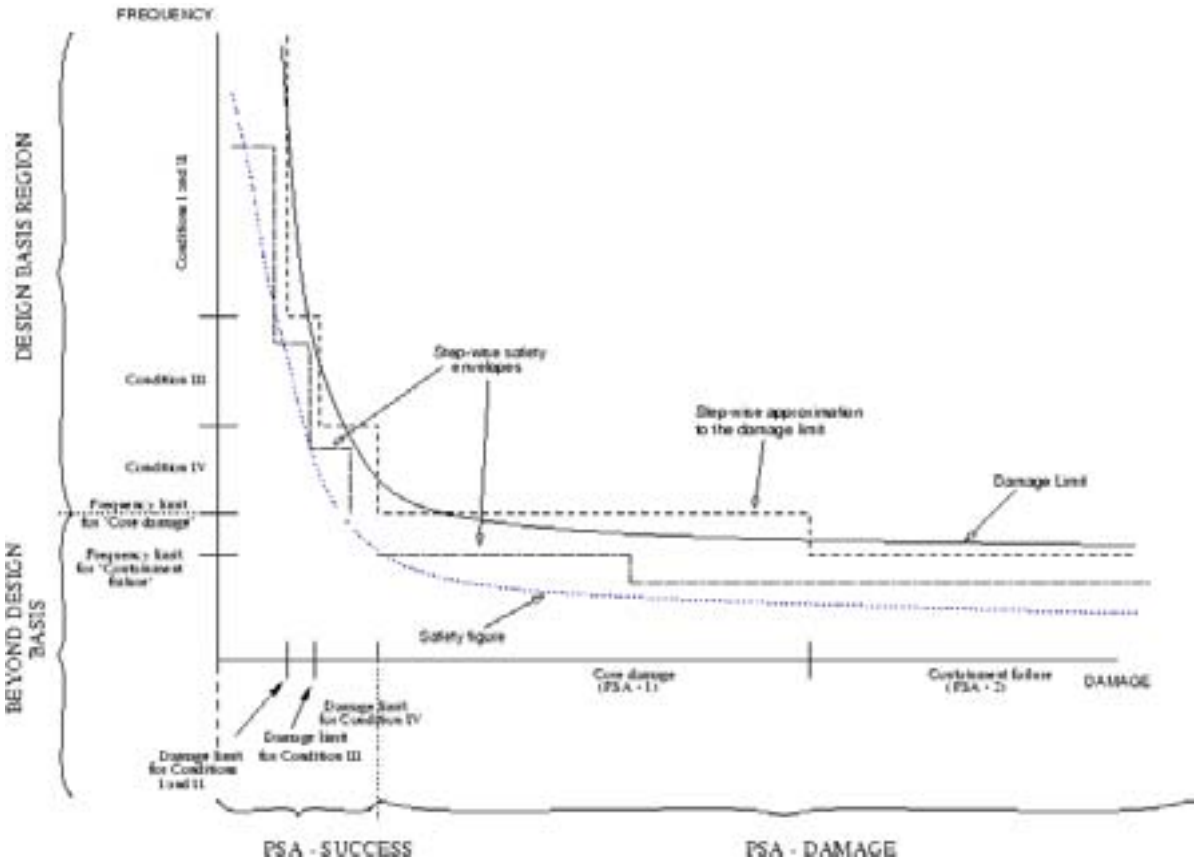


Figure 2: Illustration of the safety analysis methods

Any of these sequences gives a point of the safety figure defined by expression (6)and represented in Figure 2 by the dotted line. The coordinates are the maximum damage generated during the sequence and the **exceedance frequency** of that damage, i.e. the collective frequency of that sequence and all the sequences that generate higher damage.

The step-wise damage limit qualitatively describes the focus and objectives of *deterministic* and *probabilistic* analyses. Its projection on the vertical axis defines the frequency ranges of "design basis" (divided in *Conditions*) and "beyond design basis" transients. For each *Condition*, represented by a rather wide interval in the "design basis" region there is a well defined damage limit. On the other hand, the projection on the horizontal axis defines the ranges of PSA-success and PSA-damage, the latter divided according to the PSA levels. For each PSA level there is[11] a well defined frequency limit.

The *deterministic* approach, which is the approach of the design, necessarily must be based on a reduced number of design basis events. It consists of replacing the safety graph $\nu(D_i)$ by the step-wise safety envelope (see section 0) represented in Figure 2 by the dash-dotted line. Each step represents the set of design basis transients of the corresponding *Condition*, and the line has the following characteristics:

- The height of the step platform over the lower limit of the *Condition* is the estimated collective frequency of the DBTs, that include all the possible real transients represented by them. Note that this height can be of any magnitude in the range of the *Condition* and,

[11]It would be more appropriate to say "there could be" since this limit is not actually defined.

therefore, there is room for an error margin in the estimation. The accuracy of the estimation becomes much less critical when the damage limit and the safety graph are more vertical.

- The vertical segments of the steps, whose abscissa is the maximum calculated damage of the design basis transients, should cross the ordinate of the lower limit of the *Condition* at or to the right of the safety graph curve. This way, the calculated damage of the DBEs is assured to be an envelope of the damage of all the transients grouped in that *Condition*.

The design basis transients are assumed to represent all the transients belonging to its *Condition* where the demanded protective function works correctly. They do not represent transients where the challenged safety function fails or transients where more than one protection actuation has been required. This restriction dramatically reduces the number of transients to be taken into account and it is supported by the single failure criterion. Let us consider a DBE classified in a given *Condition*. It will challenge a particular protective function. If the function does work, the damage will be lower than or equal to the damage envelope of its *Condition*. If not, the damage will overpass the envelope and will fall in the range of a higher *Condition* or in the "beyond design basis" region. If the contribution of the resulting sequence to the frequency of the final damage range is negligible, the sequence can be ignored. This is the condition for the validity of the single failure criterion.

In the "beyond design basis" region, the PSA approach can also be described by the step-wise safety envelope (dash-dotted line). The estimated damage generated by each sequence is used only for classification in the corresponding damage range. In consequence, it can be assumed, without affecting the results of the analysis, that all the sequences classified in the same range will produce the same amount of damage and the assigned amount can be any value inside the range. The collective frequency of all the sequences classified in a range gives the height of the step whose vertical segment falls in that range and this vertical segment can be placed anywhere inside the range. The ordinate of the higher step platform is the collective frequency of all the sequences classified in this and upper ranges, i.e. the result of the PSA analysis.

It can be seen, therefore, that the damage ranges in PSA play a role analogous to the *Conditions* in the design region. i.e. they allow to classify high damage sequences as "Core damage" or "Containment failure" as a way to select the applicable frequency limit. Since the ranges are rather wide, the classification is possible even if the damage is not accurately calculated.

10. CONSISTENCY AND COMPATIBILITY OF SAFETY ANALYSIS METHODS

The developments of both concepts of safety analysis have been quite independent from each other. This means, among other things, that there could be lack of consistency or compatibility between them. However, from the previous sections we can conclude that the convergence is possible and that both methods are complementary.

In order to assure the complementarity of both methods, it would be necessary to clearly define separate fields of application for them. A frequency boundary between "design basis" and "beyond design basis" is represented in Figure 2. The region above this boundary is the application field of the *deterministic* analysis. Analogously, there is a damage boundary between "PSA-success" and "PSA-damage" regions. The application field of the *probabilistic* analysis would be the area to the right side of this boundary. A necessary condition to avoid contradictions between *deterministic* and *probabilistic* methods is that both application areas

must not overlap. In other words, the frequency limit for "Core damage" must be lower than or equal to the "design basis" boundary and the damage limit for *Condition IV* must be lower than or equal to the "PSA-damage" boundary. The case of equality in these conditions guarantees the completeness of the safety analysis.

The separation of the application fields does not imply that both methods cannot benefit from each other. *Probabilistic* techniques allow for checking the reliability assumptions made in the *deterministic* analysis. For instance, the assumption of very low failure probability, which is behind the single failure criterion, can be assessed by applying fault tree models to the protection assumed in a design basis transient.

On the other hand, the use of simulation techniques can be applied to assess the delineation of the event trees. This allows to confirm the classification of a sequence with respect to the expected damage or to find non intuitive header combinations. This kind of techniques are already used to some extent in current PSAs.

The separation of the respective scopes of the methods does not imply either that there is no interaction between them. The separation is only possible because each method implements assumptions based on the existence and particular characteristics of the other. Any change in the models or inputs associated to a safety analysis method, may alter the validity of some models or assumptions of the other method. For example, a change in the setpoint of some protective function primarily affects the *deterministic* analysis; however, that change might also have the effect of changing the protective function to be requested in a particular situation, which affects the delineation of some event trees in the *probabilistic* analysis. Similarly, any change that affects the failure probability of a protective function in the *probabilistic* analysis (for instance a change in a surveillance test interval), could invalidate the assumption that any failure sequence in the *deterministic* analysis can be ignored because of its negligible contribution to the safety envelope.

Once the complementarity of the methods and the possibility of interactions between them have been recognized, any evaluation of licensing issues supported by a safety analysis must consider both aspects of the problem. Even if the problem is clearly located in the "design basis region", i.e. it is supported by a *deterministic* analysis, there should be a check of the assumptions and inputs of the *probabilistic* analysis. The same is true in the opposite way: any licensing issue supported by a *probabilistic* analysis must include a check of the validity of potentially affected assumptions of the *deterministic* analysis.

This conception of the safety analysis gives the fundamentals to implement the philosophical principles stated in the literature about risk-informed regulation that were mentioned in the introduction to this document.

REFERENCES

[1] USNRC, "Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decision-making: General Guidance," Chapter 19 of the Standard Review Plan, July 1998.

[2] USNRC, "Regulatory Guide 1.174: An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis". July 1998.

[3] ANSI 51.1/ANSI N18.2-1973, Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants.

[4] Izquierdo, J.M. et al., Automatic generation of dynamic event trees: a tool for integrated safety assessment (ISA). *NATO ARW on Reliability and Safety Assessmen*t, 24-28 August 1992, Kusadasi, Turkey, Springer Verlag, Berlin, 1994.
[5] Izquierdo J.M., Villadóniga J.I., Importancia del análisis de transitorios en el procedimiento de autorización de reactores de agua ligera. JEN-429. Junta de Energía Nuclear, Madrid, 1979.

REGULATORY REQUIREMENTS ON THE EVALUATIONS OF SAFETY MARGINS FOR OPERATING REACTORS IN INDIA

P. HAJRA
Atomic Energy Regulatory Board,
Mumbai, India

Abstract. Atomic Energy Regulatory Board (AERB) of India requires that the safety analysis should assure that the adequate safety margins are available in the values so evaluated from the acceptance criteria or safety limits as established for the parameters under considerations. These are verified for compliance, while reviewing safety analysis reports for regulatory clearances for new reactors and proposals for changes in design, Technical Specifications, safety significant procedures etc. in the operating plants. The safety documents specify the requirements and parameters for which safety margins are to be evaluated. These parameters include limits on reactor coolant system pressure, linear heat rating of fuel, fuel temperature, clad temperature, fuel enthalpy, clad strain, extent of clad oxidation, percentage of fuel failure, hydrogen generation in containment, containment pressure and temperature, radioactivity releases to environment and radioactive dose to the public. The requirements with regard to the approaches and methodologies to be adopted for the determination of safety margin, specify that, while generally conservative analyses be made relating to transient and design basis accidents, the best estimate analysis should be followed to represent realistic scenario for the low probability events and for operating plants. For the best estimate analysis, Regulatory Body requires determinations and implications of uncertainties in calculation methods, instrument response characteristics, or other indeterminate effects in the evaluation of results. Initial conditions and assumptions should characterize all parameters including power distribution, reactivity coefficients, shutdown mechanism insertion profiles, trip settings and delays, instrumentations sensitivities and errors, off-site power availability, operability of components and systems with environmental effects, residual heat, operator action, computer codes and their validations, applicability and limitations. The paper also makes a reference to the requirements of evaluations of probabilistic safety margins to support deterministic analysis as applicable, for regulatory decision-making. Some case studies are presented to illustrate the practices with evaluation of safety margins and regulatory decision-making in safety issues of the operating reactors in India. The paper concludes with the need to standardise methodology of evaluating safety margins and establishment of acceptance safety criteria/limits for both deterministic and probabilistic evaluations.

1. INTRODUCTION

Safety margins are the differences in physical units, generally or qualitatively between the accepted established safeties criteria/limits of parameters under considerations associated with the failures/changes from the actual values worked out on account of above failures/changes. The **safety limits** usually refer to limits for which plant is designed based on codes and standards and for safe plant operations. Exceedence of these limits will require regulatory clearance before resumption of plant operations. These safety limits are specified in the Technical Specifications (Tech. Specs.) safety document of plant operations. Whereas, **safety criteria** generally refer to **acceptance criteria** for design basis accidents (DBAs). The safety limits and safety criteria for a parameter are usually same but could be different depending on the events considered and the country's policy. The regulatory acceptance criteria for the AOOs and DBAs could be more restrictive or same as safety limits/criteria. For the purpose of evaluating safety margins, **regulatory acceptance criteria** should be taken as reference.. The safety margin should be in the safer direction adequately. The safety documents stipulate these requirements for compliance. The parameters and their established or accepted safety criteria/limits to be considered for safety margin assessment will be governed by the category of events, type of anomaly or undetected defects, test or procedures under considerations. Depending on the parameters and events considered in the analysis for safety margins regulatory body may specify requirements for the **minimum safety margin**. Although emphasis is more focussed on deterministic analysis, current trend requires

compliance with **probabilistic safety targets**/ criteria, for **risk informed**/based **regulatory decision-making**.

The methodology followed in the evaluation of safety margin is the available state-of-the art technology. The approach generally comprises conservative and best estimate analysis with calculations for uncertainties indicating the confidence level in the results of the analyses. The established safety criteria/limits vis-a-vis analysis results form the basis for decision making affecting licensing for new reactors and proposals for continued operation for operating reactors. The practices and experiences on the evaluations of safety margins and regulatory decision making in India are highlighted below:

2. METHODS/APPROACHES

The methodology followed in the evaluation of safety margin is the use of the state-of-art technology either commercially available or developed in-house. Numbers of computer codes/packages are being used by the utility, reviewer, research and academic institutions. To mention some are ATMICA for blowdown and energy release related to LOCA and PACSAR, CONTRAN etc for containment analysis. These packages as per regulatory requirements or otherwise have been validated against experimental results, experiences from other plants and/or benchmark calculations on national and international levels. Regulatory Body requires documentation on details of validations and drafted a safety guide to include these aspects.

The approach practiced is generally conservative analysis for regulatory consents (licensing) of construction, commissioning and operation of new reactors and for design changes of existing operating reactors. The best estimate analysis are recommended for operating reactors seeking continued operation with undetected defects, anomaly, changes in technical specifications requirements, specific test or procedures of safety significance. Depending upon the issue, conservative analyses may also be performed for operating reactors. The best estimate analyses should generally be supported with calculations for uncertainties from modeling/methodology, use of experimental database not globally supported, instrument response characteristics and other indeterminate, and confidence level in the results of analyses. The approach to calculate uncertainties for thermal hydraulic codes used may vary. One approach may use a combination of expert judgement, statistical techniques and multiple code sensitivity calculations to combine uncertainties in key parameters, accident initial and boundary conditions and scaling effects. The second approach may use scaled experimental data and code-to-data comparisons to estimate uncertainties in predicted plant behavior. The third approach uses bounding calculations. Depending upon the issue, uncertainties addressed in gross qualitative manner may also be acceptable to the Regulatory Body. The assumptions, initial conditions including supplementary failure considerations and characterizations of all parameters including power distribution, reactivity coefficients, shutdown mechanism insertion profiles, trip settings and delays, instrumentation with their sensitivities/error bands, off-site power availability, operability of systems, structures and components, including computer based systems with environmental effects, residual heat and operator actions should be comprehensive.

3. PARAMETERS AND THEIR ACCEPTANCE SAFETY LIMITS/ CRITERIA

The most important parameters for which safety margins are evaluated relate to protection against radiological release. The consideration of any specific parameter for the evaluation will be governed by the category of events considered undetected degradation,

anomaly, and nature of changes sought in design, testing or procedures, of the operating reactors.

3.1. Deterministic safety margins

The list of such parameters include reactor coolant system pressure, minimum shutdown margin, linear heat rating of fuel, fuel temperature, clad temperature, Departure from Nucleate Boiling Ratio (DNBR), fuel enthalpy, clad strain, extent of clad oxidation, percentage of fuel failure, hydrogen generation in containment, containment pressure and temperature, and radioactive dose to the public.

The acceptable value or limit on each of these parameters is generally specified by the Regulatory Body. In cases, where not specified, utility should establish such value and evaluate to show adequate safety margin exists to support its application. **Annex 1** gives the typical safety limits/criteria for different operating plants in India. The list is not exhaustive in particular for DBAs.

3.2. Probabilistic safety margins

Of late, PSA insights are increasingly sought where applicable, by the Regulatory Body, in keeping with international trend and to supplement the deterministic safety margins. The **probabilistic safety margins** so evaluated with PSA insights with reference to the established probabilistic safety goals (targets) support and supplement deterministic analyses, technical judgement and experiences to arrive at risk informed regulatory decision. However, in some countries these are used as sole basis for decision-making where these goals could be called as **probabilistic safety criteria** for **risk based decision-making. Annex 2** gives the list of probabilistic safety goals proposed for the use after review by an expert committee to be constituted soon by the management. Although some of these are in use by many Regulatory Bodies, these are still evolving. An international consensus in this regard may be desirable and help member states to encourage use of PSA insights and provide defense-in-depth in safety assessment for decision-making.

4. ANALYSIS RESULTS AND DECISION-MAKING

With this background few case studies are presented to illustrate how regulatory decision-making process was affected with assessment of safety margins in different operating reactors in India.

Case 1: Containment peak pressure following LOCA in KGS

Kaiga Generating Station (KGS) is a twin unit 235 MWe each, of pressurised heavy water reactor (PHWR) type having double containment. The Primary Containment (PC) is designed for 1.73 kg/cm^2 (g) based on Main Steam Line Break (MSLB) and estimated for peak pressure of 1.06 kg/cm^2 (g) following LOCA. However, during safety review for authorisation of continued plant operation, it was noted that the radiological release calculations were done using 0.85 kg/cm^2 (g) as peak pressure following LOCA although for leak tightness specification for construction/commissioning 1.06 kg/cm^2 (g) has been stipulated. Utility was asked to give conservatism in the analyses and establish safety margin available in the pressure calculations. The extract of analysis is presented in the Table 1 given below.

Table 1. Containment pressure Analysis following LOCA for KGS

	Original (1987)	Current (Oct. 1999)	Remarks	Regulatory Criteria
A. Modeling assumptions/inputs				For Integrated leakage rate testing (ILRT) 1.06 kg/cm$^{2;}$ For In-service leak rate testing 0.36 kg/cm^2
Internal surfaces; m^2 Concrete Steel	24950.0 3	33787.0 5982.0	More realistic numbers used currently	
Nodalisation of containment volumes (No. of Nodes)	3	10	Latter is more realistic	
Heat transfer coefficient for containment atmosphere structures	Tagami	Diffusion Based condensation	Latter has better scientific basis; qualifies in validation exercises	
LOCA blowdown discharge model	Simple Vessel Model	Thermal Hydraulic code ATMIKA	Latter is technically more appropriate	
B. Peak pressure kg/cm^2 (g) with different bypass V_2 area 1. 1 Sq. ft* 2. 10 Sq. ft*	1.069 1.069	0.874	1.06 kg/cm^2 pressure retained for containment specifications	
C. Parametric studies 1% increase in energy 2% decrease in Volume 5% decrease in Volume*	1.107		}Not significant }effect	

* Calculated by CONTRAN code package also from reviewer side

Calculations by other code CONTRAN showed good agreement, for one case, which seemed more relevant and some variations in other cases. Since practices in some countries (eg. US, FRG, slovak NPPs (WWER)) are to add some margin in the input parameter for conservativeness, which were not used in these calculations, the Regulatory Body asked the utility to do radioactive dose calculations using 1.06 kg/cm^2 (g) peak pressure to show that adequate margin is available from acceptable regulatory limit. Since proof testing done for structural integrity during construction/commissioning stage at design pressure only, utility was also asked to calculate ultimate load bearing capacity of PC to show margin available from design value. The doses calculated thereafter with containment pressure of 1.06 kg/cm^2 (g) were much lower than acceptable limits.

Case 2: TAPS core shroud Analysis

Tarapur Atomic Power Station (TAPS) belonging to Boiling Water Reactor (BWR) type has twin reactors each de-rated to operate on single primary cycle with reduced power upto160 MWe. It's secondary steam circuit is being used as a 'dummy' recirculation line following tube leaks in secondary steam generator.

Due to reported core shroud (Material: AISI Type 304/304L) weld cracks in overseas BWRs during 1990-1995 in the lower region of core shroud welds, which were mostly circumferentially oriented and primarily due to inter-granular stress corrosion cracking, safety concern was raised for continuing operation of TAPS. Core shroud inspection done although

to limited extent in earlier inspections and immediately on unit 2 in 1998, did not show presence of any crack. To consider the issue of continuous operation till next inspection schedule, assuming presence of undetected crack, Regulatory Body wanted the utility, somewhat in the line to USNRC requirement to show adequate margin in structural integrity of core shroud was there so that under postulated event like MSLB or Re-circulation Line Break (RLB) or SSE with presence partial or 360^0 through circumferential crack, safety functions such as shutdown capability (by control rod (CRD) movement, liquid poison injection) and emergency core spray injection are not disrupted. Schematic diagrams of reactor are given in Figs.1-4. The results of the thermal hydraulic analysis (code used: RELAP4/Mod 6) and structural assessments showed that adequate margin were available for structural integrity and for safety functions required for safe shutdown and emergency core cooling under normal operating condition and postulated accident conditions of RLB, MSLB or SSC, with following conclusions:

(i) Detailed structural analysis established that even there was a complete failure of critical welds, than also there would not be any significant displacement of core shroud due to support offered by stabilizer pins.

(ii) The probability of failure of stabilizer pins is estimated to be 1.0E-11. Dynamic analysis (code used Fluidyn-NS) done considering acoustic load showed structural deformations are small in magnitude (<0.5 mm. i.e. 0.02″).

(iii) Considering crack growth rate of 5E-05 in/hr (as per USNRC core shroud studies), crack would grow due to stress corrosion cracking to about 1^0 per reactor operation year. This rate of growth was too small to cause a significant change in crack size between two or even multiple In-Service-Inspections (ISIs).

(iv) In case of critical weld failure (at H-10), resulting in failure of stabilizing pins and causing maximum lift of 9/16″ and the maximum relative displacement between top grid plate (TGP) and bottom grid plate (BGP) under RLB (which could cause higher loading than MSLB from thermal hydraulic considerations) was analysed to be less than 0.01″. Also, the maximum lateral shift between TGP and BGP with 360 degrees through wall crack at the H5 critical weld under seismic loading of SSE levels (64g horizontal and .2g vertical) was 0.0896 inches. These were well below the allowable displacement of 0.1″. Therefore, it would not affect safety functions namely control rod movement, availability of poison injection and emergency core spray.

Regarding uncertainties of the analyses, the issue was addressed as follows: The thermal hydraulic computer program had two types of correlations (a) best estimate and (b) licensing correlation. The second type, licensing correlation was used in the analyses and the predicted values were expected to be conservative. For structural assessment the ASME code was used which used minimum yield and tensile strength values. Further the TAPS core shroud was of better material properties. In view of above, uncertainty analysis was not carried out. Regulatory Body accepted the analyses for continuing operation, however desired that the probabilistic assessment (safety margin) should be made addressing change in core damage frequency due to postulated failure of core shroud.

Case 3: Anomaly in fuel sub-assembly outlet temperatures in FBTR

Fast Breeder Test Reactor (FBTR) designed for 40 MWth is the sodium cooled fast reactor presently licensed to operate up to 15 MWth. It has a core cover plate mechanism (CCPM) kept at 15 mm position above the top of fuel assemblies. The CCPM carries thermocouples (TCs) to measure fuel sub-assembly outlet temperatures. During a fuel handling campaign, CCPM got stuck first in July 1995 at higher position. With some efforts it could be brought down to its normal position. However in July 1996, after a fuel handling campaign, when normalising CCPM from its top position (80 mm.) it got stuck again. Please see Figs. 5-8.

Efforts to bring it to back to normal position were in vain. Subsequently reactor was operated with CCPM stuck at 80-mm position. However immediately after reactor power operation it was observed that outlet temperature of all sub-assemblies (SAs) were reading 10^0 less except the 26th Mark II SAs (having slightly higher fissile content) loaded in ring 3 (03-18 position) showing around 50% higher than normal. Subsequent investigation and analyses established that there were no flow blockages in the SA, and due to CCPM new position there was a skewing effect in the temperature distribution. After normalising neutronic channel power with thermal power and other SA outlet temperatures with regard to central SA temperatures, all SAs temperature estimation were 2% higher generally. However, the new SA loaded in the third ring continued to show 41% higher than the expected value. The change in new CCPM position had caused change in flux distribution in upper plenum. Although, small power changes in SAs were reflected, sensitivity for plugging detection limit in SAs seemed to have gone down. Therefore Regulatory Body directed the utility to show adequacy in margins for continued power operation by doing a 3D thermal hydraulic analysis in addition to other investigations and also the probability of flow blockage was less for acceptability.

3D analysis indicated that the clad hot spot temperature was 608^0 C well below the allowable value of 700^0 C. The flow through SA at central position was normal and temperature read at 80 mm position was capable of detecting plugging above 30% (60% plugging would result in increase in SA outlet temperature of 10^0 C, which could well be detected by TCs and plugging detection sub-routine), and the tolerable design plugging limit was 72%. Any undercooling of Mark I assembly would be detected by TC readings. Further, the probability for flow blockage in SA was estimated to be 5.5 E-03/RY and probability for flow blockage without safety action, 6.6E-07/RY, which was lower than acceptable value.

Case 4: Probabilistic Analysis: NAPS/KAPS/TAPS

This illustrates evaluation of probabilistic safety margin and decision-making for continued reactor operation. Recently, regulatory policy was drafted to use PSA insights including uncertainty analysis to support and supplement deterministic analyses and engineering judgement for risk informed decision in all the areas where PSA results could be considered useful such as: Changes in Tech. Specs. Clauses relating to Allowed Outage times (AOTs), Surveillance Test Intervals (STIs), design modifications, configuration management etc. In this regard, suggested probabilistic targets given in **Annex 2** could be again referred to. One of the requirements for renewal of license for continued operation is to show that the reliabilities of safety structures, system and components have not degraded from the target values as provided in the safety reports of the plant. **Annex 3** gives target reliabilities of a typical 220 MWe PHWR plant. Based on review of such submission, the Regulatory Body asked Narora Atomic Power Station (NAPS) to take measures for better performance of

MOVs, TAPS to improve the reliability of Class III power supply, which is the dominant contributor for unavailability of Core spray and Post Incident systems.

Presently, the proposal of Kakarapar Atomic Power Station (KAPS) for change in surveillance test frequency of emergency diesel generators from weekly to monthly if failure rate (FR) < 1 in last 100 tests, to fortnightly if FR = 2 in last 100 tests and to weekly if FR = 3 for last 100 tests, is under review with PSA insights, to assure adequate probabilistic margin is available for decision-making.

5. CONCLUSIONS

In conclusion the following are put forward:

1) Determination of safety margins both deterministically and probabilistically including considerations of uncertainties as applicable, in safety assessment is important for regulatory decision making.

2) The practices followed in the approach and methodology may vary with the issues under considerations and from country to country.

3) The parameters and their values with regard to the safety limits/acceptance criteria in deterministic analysis are likely to be different depending on reactor type and design and country's policy. The parameter and their values for probabilistic safety criteria will not vary significantly with reactor type and design, except with country's policy. Hence, a common standard could be evolved.
4) A safety document recommending standard methodology to be used including supplementary failure postulations and widely accepted use of computer packages, for performance of specific tasks, together with acceptance criteria, for deterministic and probabilistic evaluations of safety margins, would be very useful.

ACKNOWLEDGEMENT

I am also thankful to my colleagues S/Shri. R. B. Solanki, R. Srinivasa Rao and Harikumar who helped me in preparation of this paper.

Annex I

Deterministic safety limits*/criteria# for operating plants in India

Reactor	Parameters	Value
BWR	1. Fuel clad integrity (NO & AOO)	1.Reactor thermal power to water shall not exceed specified limits when reactor pressure is greater than 600 psig (42.18 kg/cm2) 2.When reactor pressure is less than 600 psig, the reactor thermal power shall not exceed 129 MWt 3.Whenever reactor is in shutdown condition with irradiated fuel inside, water level shall not be less than 59" (149.9 cm) above the top of fuel 4.The neutron flux shall not be above scram settings
	2. Reactor coolant system (RCS) pressure (NO & AOO)	The RCS pressure shall not exceed 1375 psig at the bottom of the reactor vessel
	3. Clad integrity (DBAs)	Should not reach local clad melting
PHWR	1. PHT system boundary integrity (NO&AOO)	PHT pressure should not exceed 107 kg/cm2 (Kaiga) 101 kg/cm2 (RAPS 1&2)
	2. Fuel Clad integrity (NO&AOO)	The rating of any fuel element shall not exceed òkdq value of 46 W/cm (bundle power 483 kW)
	3. Loading on fuel (NO&AOO)	Maximum compressive load in a fuel bundle shall not exceed 1000kg (RAPS 3&4,KGS, NAPS, KAPS) 545 kg (RAPS 1&2, MAPS)
	4. Clad temperature (DBAs)	8000C 12000C not more than 60 s
	5. Fuel enthalpy limit (DBA)	840 kJ/kg
	6. Clad oxidation (DBAs)	17% of original clad thickness or oxygen concentration above 0.7% by weight in half clad thickness
	7. Fuel centerline temperature (DBAs)	No melting
	8. Coolant channel geometry (DBAs)	Should remain coolable
	9. Containment pressure, H_2 concentration (DBAs)	Containment peak pressure should be below design limit, H_2 concentration should not reach deflagration limit or detonation limit
FBTR	1. Fuel thermal behaviour (NO & AOO)	The operating linear heat rating (LHR) shall be limited to 480 W/cm ensuring that none of the assemblies exceeds its operating limit on LHR taking into account its burn up, core position and fuel composition. The design safety limit (DSL) for LHR shall not exceed 373 W/cm for fresh mark I fuel and 315 W/cm for fresh Mark II fuel. For irradiated fuel the peak DSL for each subassembly shall derived from the operating history.

	2. Fuel Clad integrity (NO & AOO)	The sodium outlet temperature from any fuel subassembly shall not exceed 650^0C
	3. Primary boundary integrity (NO & AOO)	The primary sodium temperature shall not exceed 600^0C
	4. Fuel Clad temperature (NO)	700^0C
	5. Fuel Clad temperature (AOO)	800^0C
All plants	Radiological dose limit	Prescribe limit for NO & AOO :100 mR Acceptable limit for DBA : 10 Rem whole body 50 Rem thyroid

* Safety limits is for normal operation (NO) and anticipated operational occurrences (AOO).

\# Safety criteria is for design basis accidents (DBAs).

Annex II

Probabilistic safety targets

- Identification of critical components based on certain risk increase value such as 0.1% increase in CDF or 1% increase in system unavailability (suggested for sensitivity/risk importance measure studies)

- Safety and safety related systems unavailability target. For example:

1. Shutdown System ≤ 1.0E-6/demand
2. Engineered Safety Features:
   - ECCS ≤ 3.5 E-3 a/a
   - Containment Isolation ≤ 2.0 E-4 a/a
3. Class III Emergency Power Supply ≤ 1E-3/Demand
4. Fire Fighting Water system ≤ 1E-3/Demand
5. Reactor Regulating System ≤0.3Failures/a

These unavailability values of the systems are suggested considering that accident sequences resulting in core damage will be < 1.0E-5/a

- Adequacy of design and operational framework can be based on:
  (i) CDF for operating NPP: ≤ 1.0E-4/R-Y and for New NPP: ≤ 1.0E-5/R-Y and
  (ii) Limiting contribution to CDF from any dominant accident sequence < 25%

- Risk based AOT exceeding a limiting value 0.1% increase in CDF (DCDF) or 1% increase in system unavailability.Risk based STI: any change in STI resulting in increase in system unavailability by more than 1% or increase in CDF (DCDF) by more than 0.1%

- Probability of radioactivity release beyond acceptable levels from BDBAs less than a target value ≤ 1.0E-6/R-Y
- Individual risk of fatality from radiation exposure in severe accident less than a target value (1.0E-7/R-Y)

  The estimated probability of emergency radioactivity release equaling or exceeding action level requiring evacuation of personnel living beyond exclusion zone should not exceed 1.0E-07 per reactor year.

Annex III

Design targets for reliabilities of safety component/systems in PHWR plants

System/Components	Unavaibilities
Reactor Regulating System	0.3 failure/a
Large Break LOCA	1.0E-04/a
Small Break LOCA	1.0E-04/a
Reactor Shutdown System	2.0E-5/demand (a/a)
Emergency Core Cooling System	3.5E-3/demand
Class III Emergency Power Supplies	3.0E-4 to 1.0E-3/demand
Containment Isolation System	2.0E-4/demand
R. B. Coolers	1.0E-3/demand
Fire Fighting Water System	1.0E-3/demand
Main Steam Line Break	3.0E-3 failure/a
DG Set	1.35E-3 a/a
MG Set	1.1E-3 a/a
250V D.C. Battery	8.2 E-5 a/a
Unit Transformer	5.5E-5 a/a
Core Cooling System MV	1.0E-3/demand
Ventilation Damper Failure	1.2E-3/demand
Air Compressor	0.1 a/a

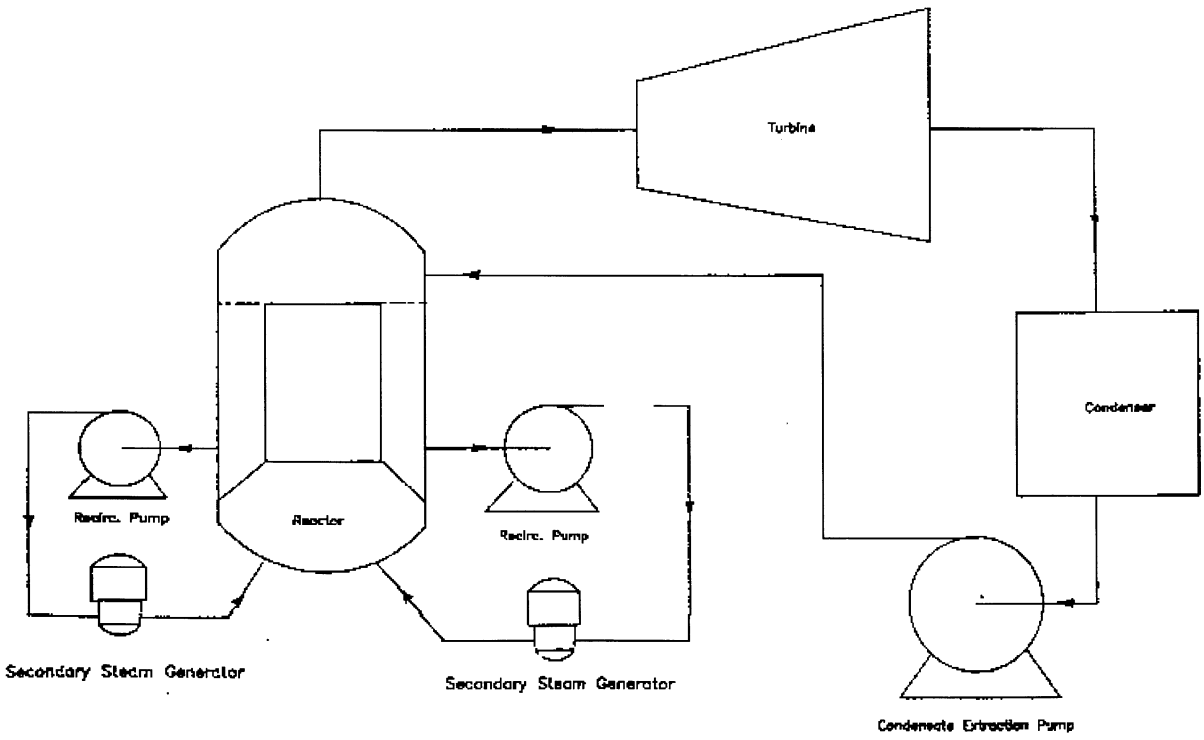


FIG. 1. Simplified schematic flow diagram of TAPS-BWR.

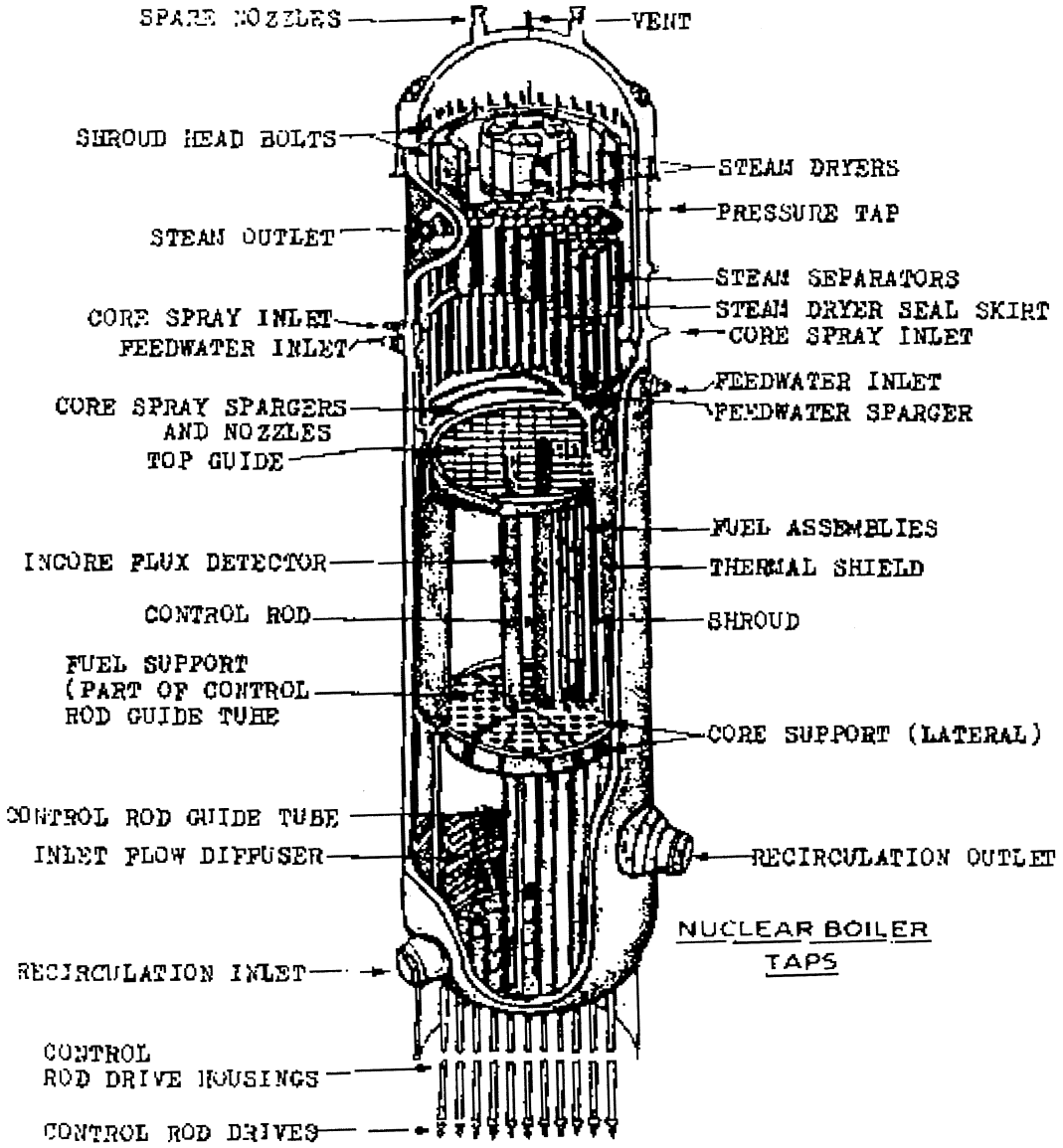

SPARE NOZZLES
VENT
SHROUD HEAD BOLTS
STEAM DRYERS
PRESSURE TAP
STEAM OUTLET
STEAM SEPARATORS
STEAM DRYER SEAL SKIRT
CORE SPRAY INLET
CORE SPRAY INLET
FEEDWATER INLET
FEEDWATER INLET
CORE SPRAY SPARGERS
AND NOZZLES
FEEDWATER SPARGER
TOP GUIDE
FUEL ASSEMBLIES
INCORE FLUX DETECTOR
THERMAL SHIELD
CONTROL ROD
SHROUD
FUEL SUPPORT
(PART OF CONTROL
ROD GUIDE TUBE
CORE SUPPORT (LATERAL)
CONTROL ROD GUIDE TUBE
INLET FLOW DIFFUSER
RECIRCULATION OUTLET
NUCLEAR BOILER
TAPS
RECIRCULATION INLET
CONTROL
ROD DRIVE HOUSINGS
CONTROL ROD DRIVES

FIG. 2.

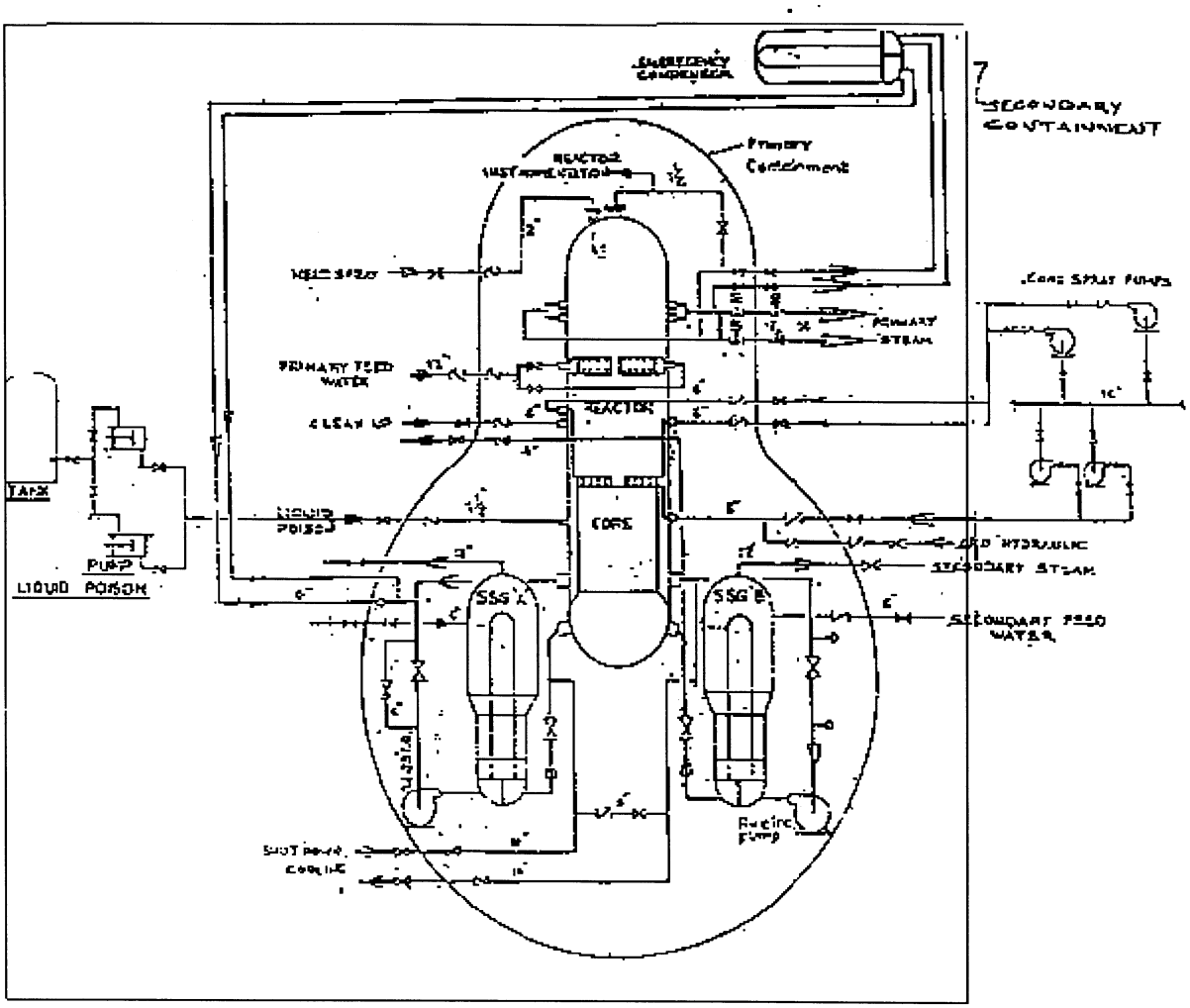


FIG. 3. TARAPUR boiling water reactor.

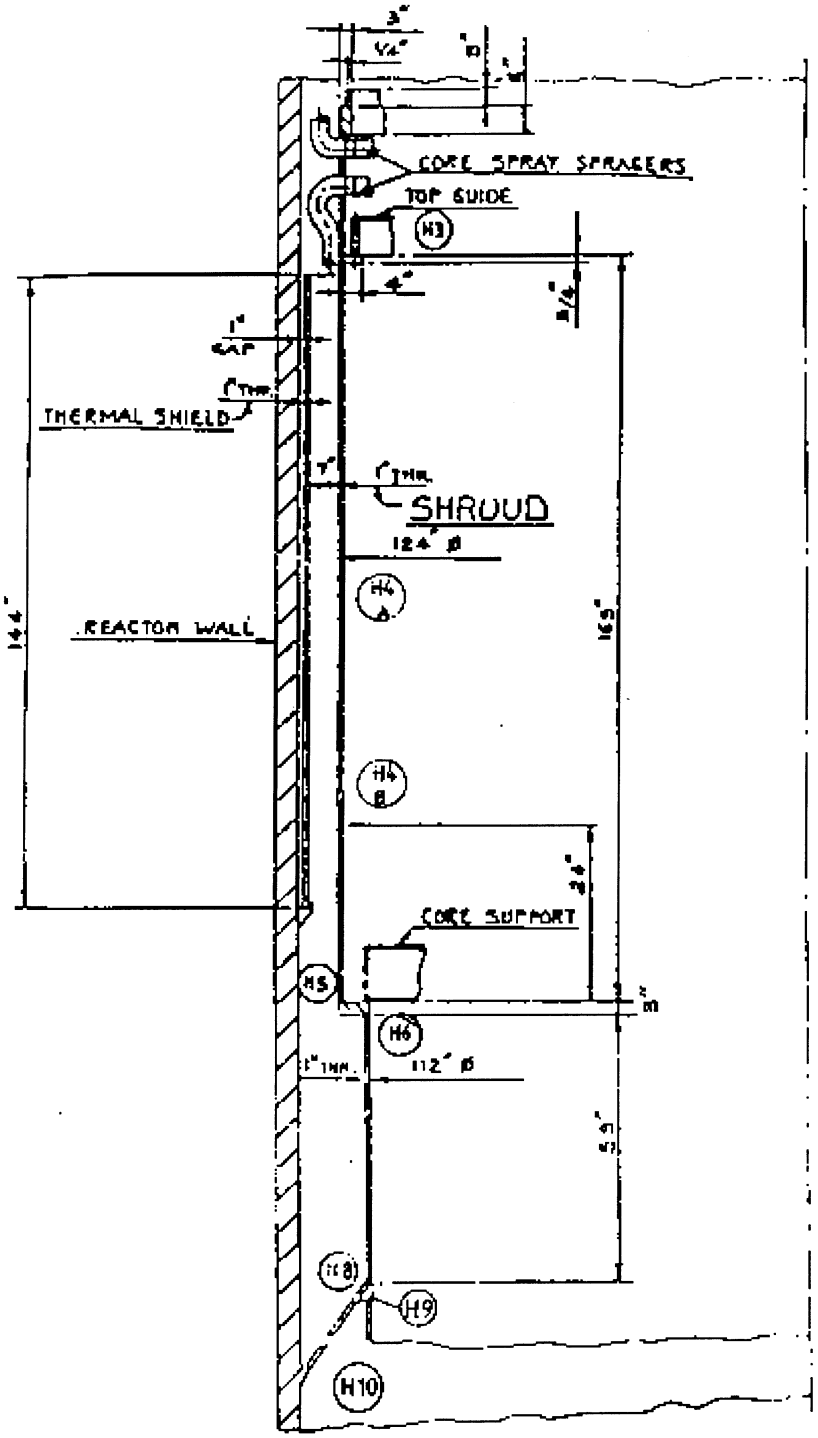


FIG. 4. TABS reactor shroud arrangement.

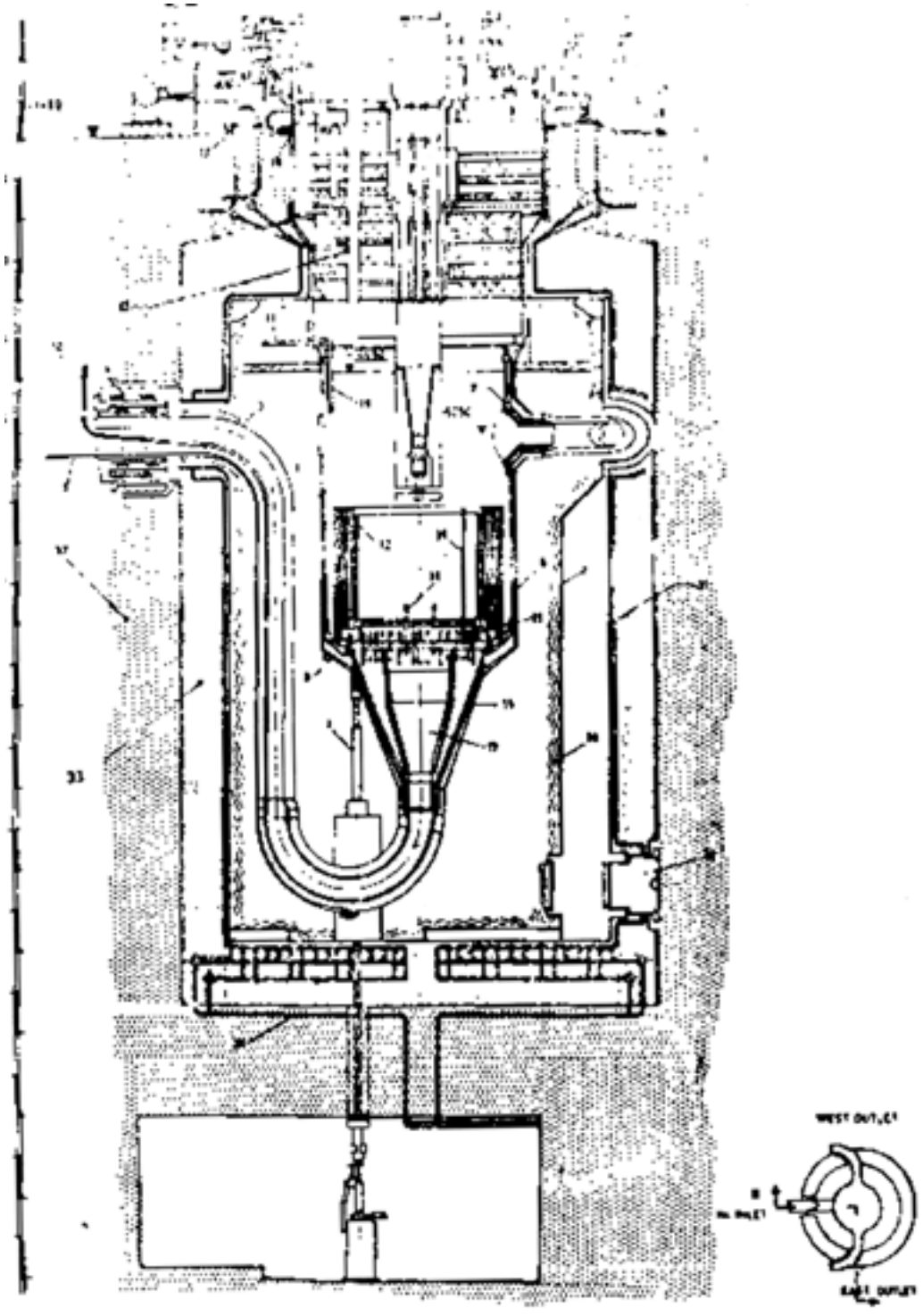


FIG. 5.

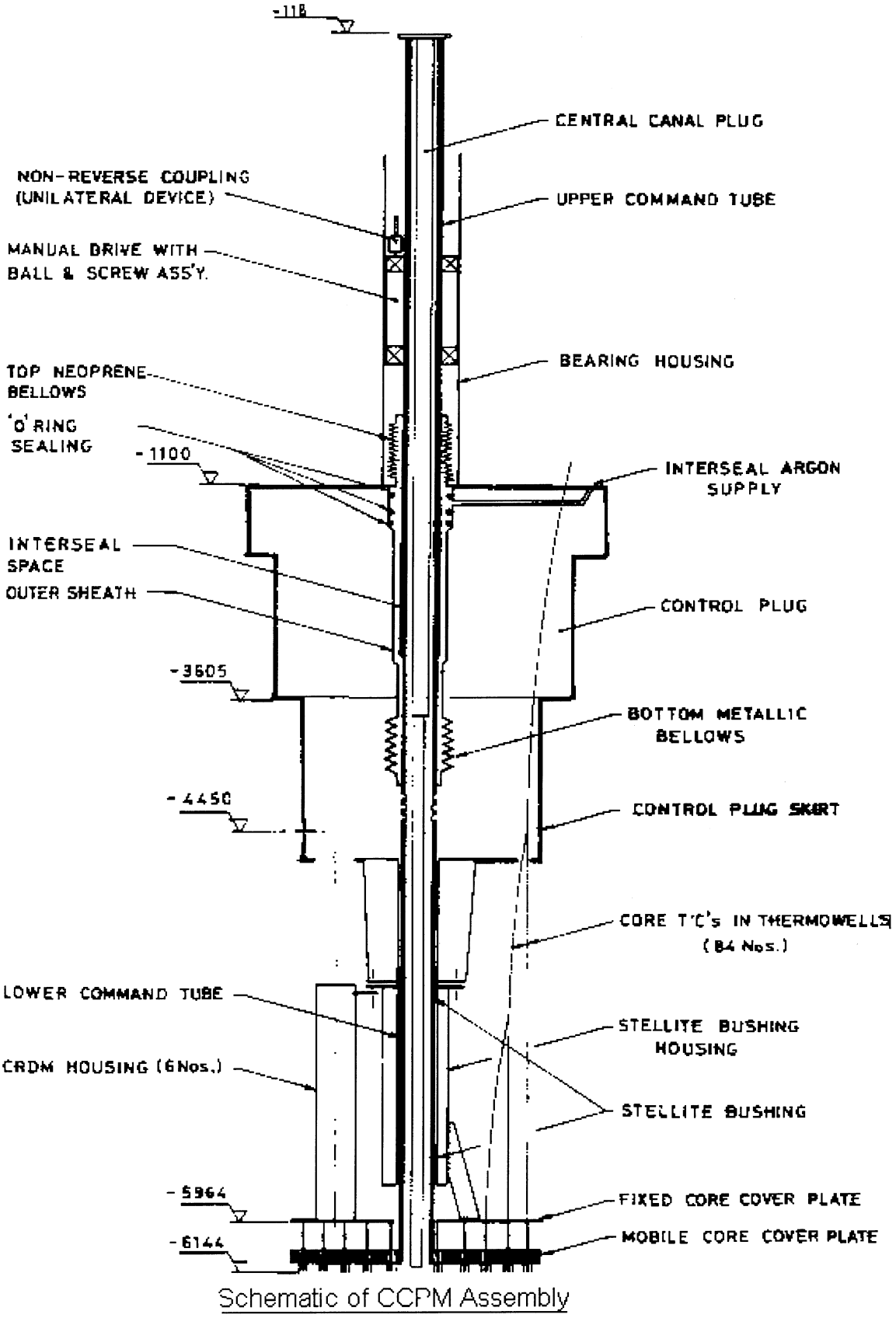

-118
CENTRAL CANAL PLUG
NON-REVERSE COUPLING
(UNILATERAL DEVICE)
UPPER COMMAND TUBE
MANUAL DRIVE WITH
BALL & SCREW ASS'Y.
BEARING HOUSING
TOP NEOPRENE
BELLOWS
'O' RING
SEALING
-1100
INTERSEAL ARGON
SUPPLY
INTERSEAL
SPACE
OUTER SHEATH
CONTROL PLUG
-3605
BOTTOM METALLIC
BELLOWS
-4450
CONTROL PLUG SKIRT
CORE T'C's IN THERMOWELLS
(84 Nos.)
LOWER COMMAND TUBE
STELLITE BUSHING
HOUSING
CRDM HOUSING (6Nos.)
STELLITE BUSHING
-5964
FIXED CORE COVER PLATE
-6144
MOBILE CORE COVER PLATE
Schematic of CCPM Assembly

FIG. 6.

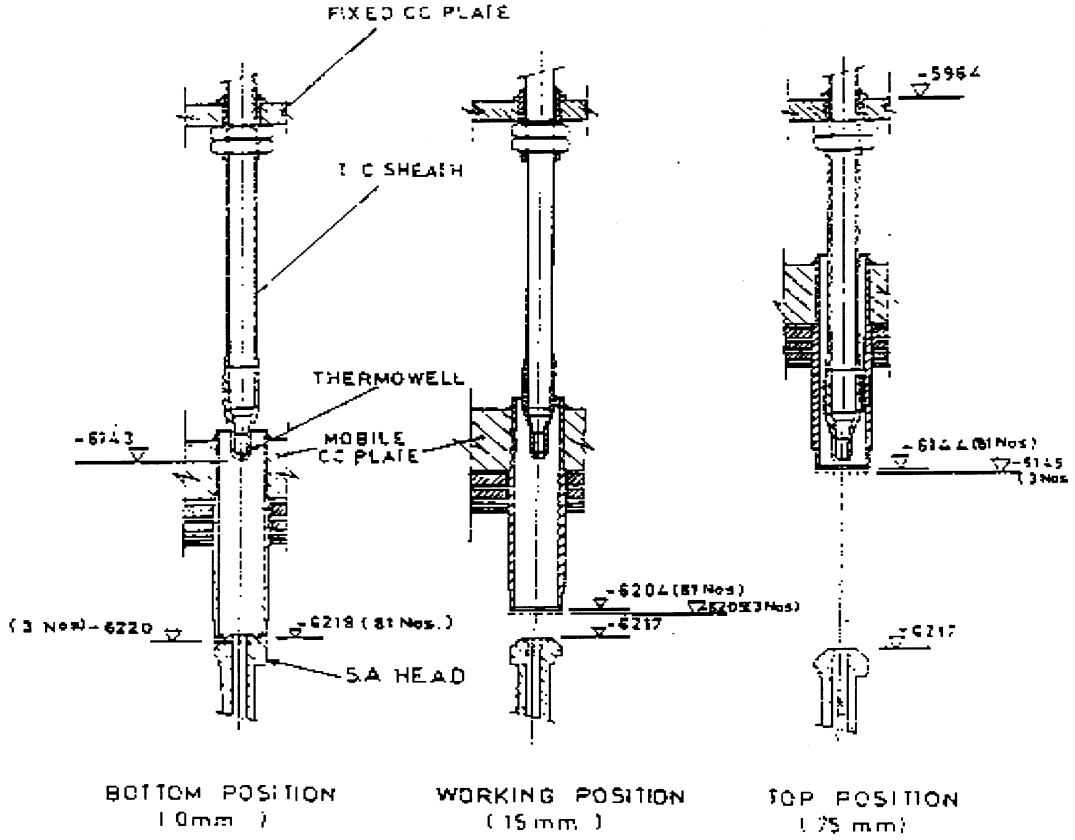


FIG. 7. Three positions of the mobile core cover plate.

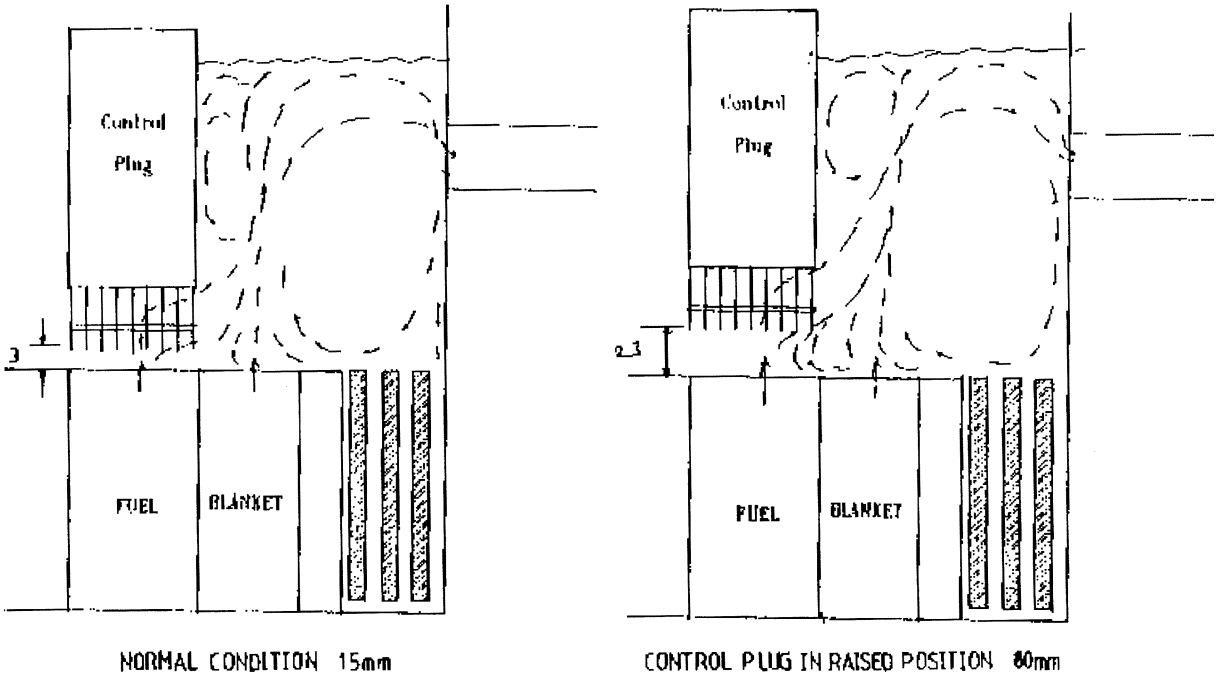


FIG. 8.

REFUELLING DESIGN SAFETY LIMITS OF PAKS NPP

I. NEMES
Paks NPP Ltd,
Paks, Hungary

Abstract. This paper lists the Safety Analysis Bounding Limits of NPP Paks. The limits cover all important reactor physical parameters of WWER-440 units. The limit table is fixed in the Technical Specification. All limits are to be satisfied taking into account uncertainty of a given parameters. Uncertainties are determined using specific treatments, specific tests or benchmark calculations.

1 INTRODUCTION

During Safety Analysis of NPP Paks a bounding parameter set of Safety Analysis Bounding Limits were established. The way of determination of these parameters were as follows:

The basis of calculations was a typical equilibrium cycle's BOC, MOC and EOC conditions with its enrichment and burnup distribution. In order to expand the validity of safety analysis calculations as far as it possible, conservative determination of neutron physical parameters were used. The sequence of this determination process consisted of two phase:

- It was chosen the set of main determining parameters (key-parameters) in each type of transient analyzed. (Let it called) Usually it was unambiguous to find some neutron physical characteristic parameters playing the main role in the determination of final results of a given analysis. (E.g. in case of control rod ejection analysis the determining parameters: the integral efficiency of the ejected rod and the feedback coefficients).

- Starting from the mentioned basis the neutron physical model was adjusted to achieve the required characteristics with respect to the key-parameters.

- The conservatism required in certain parameter has to include the followings:

- The variation of the given parameter according to different transient core design.

- Tolerance for the uncertainties for the determination of it in the refueling design practice by calculation and/or in core performance practice by measurement.

It was also required the model to remain reasonable, so the level of this adjustment was limited. On the other hand the conservatism could be limited by the acceptance criteria in the analysis (choosing too conservative inputs the acceptance criteria may not be satisfied).

In case of one key-parameter (e.g. moderator temperature coefficient) which played important rule in more then one analysis we tended to use the same conservative parameter value in different condition.

2. SAFETY ANALYSIS BOUNDING LIMITS OF NPP PAKS

Collecting systematically determined key parameters from different parts of safety analysis we got the Safety Analysis Bounding Limit table for NPP Paks units. The bounding limits have been fixed in the Technical Specification of NPP Paks, and now the goal of refuelling design calculations to prove that the given reload satisfy all criteria of SABL tables. The limits for different physical parameters are as follows:

Local power and temperature limits

Parameter	Limitation	Reactor state
Maximal linear heat rate ()	< 325 W/cm (burnup dependent)	all
Maximal subchanel outlet temperature	T_{sat}	all

Burn-up limits

Parameter	Limitation
Assembly burnup	< 49 GWd/tU
Pin burnup	< 55 GWd/tU
Pin local (pellet) burnup	< 64 GWd/tU

Limits of control rod worth

Parameter	Limitation	Reactor state
Efficiency of all control rods, except the most effective one	> 5100 pcm	all
Integral efficiency of group 6 rods (regulating group)	> 1300 pcm < 2500 pcm	all
Efficiency of one ejected rod	< 210 pcm < 730 pcm	FP HZP
Differential rod efficiency	< 0.037 $/cm	near critical

Limits on reactivity conditions

Parameter	Limitation	Reactor state
Critical boric acid concentration	< 10.5 g/kg	all (HZP)
Shutdown margin (1)	<-2000 pcm	HZP (260 C)
Shutdown margin (2)	< 0	ZP, 210 C
Minimal subcriticality during refuelling condition (the most effective follower in the core)	< -5000 pcm	Zero power, 100 C

Reactivity feedback coefficient limits

Parameter	Limitation	Reactor state
Boric acid efficiency	< -1900 pcmkg/g > -1000 pcmkg/g	all all
Moderator temperature efficiency	< 0.0 pcm/K > -70.0 pcm/K	 all
Doppler efficiency	< -2.4 pcm/K > -4.9 pcm/K	all

In addition the assembly flow rate, and the core inlet temperature are limited as well.

Uncertainty of parameters

Each parameter listed in the SABL table has to have well-established uncertainty. The list of parameters uncertainties also attached to the Technical Specification. The way of determination of these uncertainties is different for different data.

In case of the linear power, the subchanel temperature and the different burnup limits a detailed analysis have been treated to determine the uncertainty, the so-called *safety factors.* The safety factor include the result of material and geometry tolerances and the code uncertainties for the determination of a given parameter value. The code uncertainties are determined through the wide scale of different tests. In these tests calculated results were compared to measurements and to the results of Monte-Carlo and transport calculations.

For the boron concentration, boron worth, moderator temperature coefficient and some control rod worth the uncertainties of calculated parameters are approached by the deviations between the measured and calculated parameter values.

For the rest of parameters we have no available measured references. In this cases the uncertainties are determined through different international benchmark calculation in which the results of different code calculation have been compared.

The uncertainty of parameters in the SABL table of NPP Paks is as follows:

Parameter	Uncertainty
Maximal linear heat rate	39 W/cm
Maximal subchanel outlet temperature	7.5 C
Assembly burnup	7.65%
Pin burnup	13.6%
Pin local (pellet) burnup	13.6%
Efficiency of all control rods, except the most effective one	10%
Integral efficiency of group 6 rods (regulating group)	10%
Efficiency of one ejected rod	10%
Differential rod efficiency	0.00462 $/cm
Critical boric acid concentration	4.5%
Shutdown margin (1)	750 pcm
Shutdown margin (2)	750 pcm
Minimal subcriticality during refuelling condition (the most effective follower in the core)	750 pcm
Boric acid efficiency	100 pcm/kg*g
Moderator temperature efficiency	2.5 pcm/C
Doppler efficiency	20%

3. EVALUATION OF MEASURED RESULTS

During start-up after refuelling and also during the cycle some parameters are measured at NPP Paks such as:

- Critical boron concentration
- Moderator temperature coefficient
- Different control rod efficiencies
- Temperature and power distribution

The measured results in the NPP Paks practice are evaluated in the following way:

- Measured parameter result required not to exceed limit value (if such limit exists)
- Measured parameter compared to calculated one taking into account the declared uncertainty of a given data

4. SUMMARY

Safety analysis bounding limits of NPP Paks were determined systematically during SA of NPP Paks. The limit set covers all-important physical parameters of WWER reactor core. The limit values are to be satisfied during refuelling design work taking into account well established tolerances. Selected parameters are measured during start-up tests and during the cycles. The measured parameter values are systematically evaluated.

PRACTICAL USE OF UNCERTAINTY EVALUATION METHODS IN SLOVENIA

A. PROŠEK, B. MAVKO
Reactor Engineering Division,
Jožef Stefan Institute,
Ljubljana, Slovenia

Abstract. In the world the use of best estimate codes with uncertainty evaluation is increased. Also on the national level significant efforts were devoted to the uncertainty evaluation of RELAP5 best estimate computer code. Independent research and analyses have been carried out to be able to predict the Krško nuclear power plant (NPP) loss-of-coolant accident (LOCA) margins before steam generator replacement and power uprate. The Krško plant is a two loop Westinghouse pressurized water reactor type. The purpose of the paper is to present the practical use of uncertainty methods for quantifying the LOCA margins. For uncertainty evaluation the Code Scaling, Applicability, and Uncertainty (CSAU) evaluation method was used. For uncertainty analysis of large-break LOCA double ended guillotine break was chosen. Blowdown, refill and reflood phases were taken into consideration. For analysis purposes computer code RELAP5/MOD2 version 36.05 was used to calculate the peak cladding temperature (PCT) selected as safety parameter. With some drawbacks the RELAP5/MOD2 code (frozen version) was determined to be applicable for this kind of analysis. In total 128 calculations were performed. The main contribution of the work was demonstration of the applicability of the CSAU methodology for the evaluation of the specific power plant. The analysis was built on the original one [1] and was therefore considerably less costly. To show applicability of the CSAU method also to small-break LOCA the CSAU method was applied to 5.08 cm break accident scenario. The scenario was subdivided into five phases. In total 59 calculations were performed using qualified nodalization and RELAP5/MOD 3.2 code. For output uncertainty parameters three single safety parameters (including PCT) and nine system and safety continues-valued output parameters were chosen. The main contribution of this analysis was demonstrated capability of optimal statistical estimator to calculate uncertainty of both single value and continues-valued output parameters. The results indicate that the CSAU uncertainty methodology could be used for uncertainty evaluation of non-LOCA accidents.

1. INTRODUCTION

The use of best estimate codes for safety analysis requires quantification of the uncertainties. The Code Scaling, Applicability and Uncertainty (CSAU) method was developed and demonstrated to a large-break loss-of-coolant accident (LB LOCA) in 1989 by USNRC [1, 2] Later several new methods were developed in the world:

- AEAW method (Atomic Energy Authority Winfrith) [3]
- CEA/IPSN method (Commissariat a l'Energie Atomique/Institut de Protection et de Sureté Nucleairé) [4, 5]
- GRS method (Gesellschaft für Anlagen- und Reaktorsicherheit) [6]
- UMAE method (Uncertainty Methodology based on Accuracy Extrapolation) [7], and a few other

In the pioneering study of quantifying safety margins of best estimate code by Boyack et al. [2] the response surface was used for the uncertainty evaluation of the peak cladding temperature (PCT) during a LB LOCA in a pressurized water reactor (PWR) with U-tubes steam generators (SG). Regression analysis (polynomial fit) was used for the response surface generation. Next application of the CSAU was to a small-break (SB) LOCA in a PWR of different type, using the RELAP5/MOD3 code [8]. The safety parameter selected was core level and for response surface generation regression analysis was used.

The first complete application of the UMAE method was carried out for a small break LOCA (6% area) in the Krško nuclear power plant (NPP) [7]. The GRS and IPSN methods

are fully probabilistic. The first uncertainty analyses were done for the OMEGA Rod Bundle Test with the ATHLET code using the GRS method [9] and for the Vertical CANON Test with the CATHARE code using the IPSN method [4]. Other contributions were also made to various methods with limited or reduced time and resources. Applications have been made to a LB LOCA in a PWR with the RELAP5/MOD2 [10, 11] with the TRAC-PF1/MOD2 code [12] and to the BETHSY 9.1b test with the RELAP5/MOD3.1 code [13].

The Uncertainty Methods Study Group founded in the OECD/CSNI showed comparisons of several application methods developed in Europe to calculate uncertainty respecting specified parameters for the International Standard Problem [14].

Westinghouse has also begun to use W methodology based on CSAU for LB LOCA calculation. The response surfaces to fit calculational data points were used and then these response surfaces in a Monte Carlo simulation were used to generate the output distribution [15]. Recently, the Westinghouse best estimate LOCA licensing methodology based on WCOBRA/TRAC code was presented [16]. The regression analysis was used for response surface generation and Monte Carlo method for PCT distribution (the only safety parameter).

The CSAU approach was partly followed also in Japan for licensing analysis of boiling water reactor [17]. They modified the uncertainty evaluation part by establishing the distribution of safety parameter (minimum critical power ratio) and statistical upper bound of the distribution was then determined as the tolerance limit with a specified probability. The distribution was tested for the normality by the chi-squared goodness-of-fit test.

Also on the national level significant efforts were devoted to the uncertainty evaluation of RELAP5 best estimate computer code. Independent research and analyses have been carried out to be able to predict the Krško nuclear power plant LOCA margins before steam generator replacement and power uprate. For uncertainty evaluation the CSAU evaluation method was used. The simplified uncertainty analysis of LB LOCA double-ended guillotine break was published in 1992 [18].

To show applicability of the CSAU method also to SB LOCA the CSAU method was applied to 5.08 cm break accident scenario [19]. The response surface was generated by optimal statistical estimator [20] and Monte Carlo method was used for uncertainty analysis.

The purpose of this paper is to present Slovenian efforts in uncertainty evaluation. The applications of CSAU to LB LOCA and SB LOCA in a Krško two-loop pressurized water reactor, Westinghouse type, 1882 MWt power before SG replacement and power uprate to 2000 MWt, are presented.

2. APPLICATION OF CSAU TO LB LOCA

2.1. Preparation for the analysis

Scenario specification for double ended guillotine break LB LOCA was specified as described in. Blowdown, refill and reflood phase were taken into consideration. Performance of emergency core cooling was assessed with emergency core cooling system performance criteria, one of the most limiting being the PCT limit. Krško NPP located in Slovenia, a two loop Westinghouse pressurized water reactor type, was selected for analysis. For analysis purposes the RELAP5/MOD2 computer code was used to calculate the PCT. This is a frozen code version

and complete code documentation was provided [21, 22]. With some drawbacks the RELAP5/MOD2 code was determined to be applicable for this kind of analysis.

NPP Krško standard input model for RELAP5/MOD2 was used for various transient analyses [23, 24, 25]. The model was adopted to suit LB LOCA calculation. Additional heat slabs were introduced into the core to represent the axial power profile with 13 heat slabs. There were two different hot rods modelled in the RELAP5/MOD2 core model to halve the number of calculations since each hot rod had different fuel parameters. The number of heat slabs was reduced on the secondary side to save CPU time. Double-ended guillotine break was modelled in the cold leg between reactor vessel and reactor coolant pump. High and low pressure safety injection were modelled with time dependent junctions and flow versus pressure tables.

Seven parameters, that have the largest influence on PCT, were selected for the uncertainty analysis. In selecting the parameters, findings in [1,2] were used. Chosen parameters are shown in Table1. The last three parameters in the table are plant specific and were chosen based on the conservative calculations performed in the past [26]. Heat transfer coefficient was not included in the analysis because multiplier coefficient for heat transfer does not exist in the RELAP5/MOD2.

Table 1
Uncertainty parameters

Input parameter	**Uncertainty range**
Peaking factor	±5.6%
Fuel conductivity	+10%, -5%
Gap conductance	+35%, -80%
Pump degradation	see Table **Error! Bookmark not defined.**
SG plugging	0, 10%, 18%
Break size	40%, 30%
Safety injection (SI)	± 20%

Table 2: Pump
head multiplier

Void fraction	**Nominal M**	**Level 1 M**	**Level 2 M**
0.00	0.0	0.0	0.0
0.24	0.8	0.6	0.4
0.30	0.96	0.8	0.6
0.80	0.9	0.7	0.5
1.00	0.0	0.0	0.0

M multiplier

2.2. Sensitivity and uncertainty analysis

The calculational matrix with 128 elements was formed. Each element of calculational matrix represented LB LOCA calculation at selected values of parameters. For the 128 temperatures 64 calculations were necessary. Increasing fuel thermal conductivity and gap conductance decreased the PCT. Decreasing power peaking factor also decreased the PCT. Increasing plugging level slightly increased the PCT. The SI flow had no effect during blowdown because injection was delayed on SI signal.

In order to produce a good estimate of the probability function from the response surface (RS) it must be sampled in statistically acceptable way. Because the surface was only algebraic, crude Monte Carlo sampler was used. Response Surface may be established in different ways. The ones we used were Regression Analysis (RA) and Optimal Statistical Estimator (OSE). For further details regarding OSE the reader is referred to [20]. RA can be viewed simply as multinominal least squares fitting process. The purpose of both methods was to replace the code output (PCT) by a fit.

The probability distribution 95th percentile was accepted as an indication that any important uncertainties are accounted for. We were interested in knowing what fraction of the response surface exceeds any given value of PCT. For this the cumulative distribution function was needed. The procedure for obtaining it was to randomly generate seven input parameters within parameter uncertainty (see Table 1). For each parameter independent random generator was chosen. The values of parameters chosen were inserted in the fit (response surface) and PCT was calculated. This procedure was repeated many times and values of PCT were accumulated in the preselected bins (1000 K to 1010 K; 1010 K to 1020 K; etc) and normalised by the total number of trials. The result was frequency histogram interpreted as the probability distribution function. From the histogram standard statistics (mean, 95 percentile) was determined.

The final goal was the estimation of the total uncertainty of PCT. The analyses were done for blowdown and reflood phase. The results obtained by two different methods for response surface calculation of PCT for blowdown phase are shown on Figure 1. From probability distribution function the mean and 95th percentile PCT were determined as shown in Table 3. These 95 percentile PCTs were then compared to the acceptance limit (1478 K).

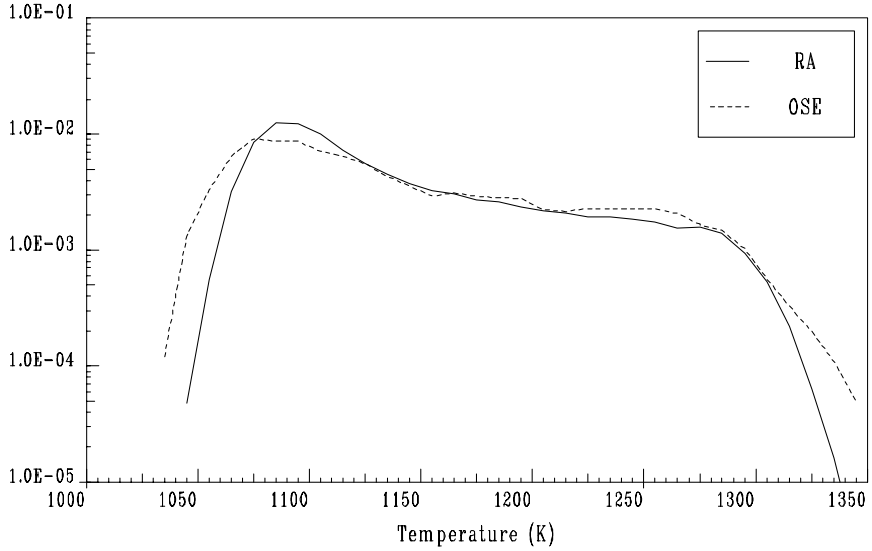


Figure 1. Comparison of the probability distribution functions calculated from RA and OSE generated response surface for blowdown phase [27].

Table 3 Statistics for peak cladding temperature

Model	**Peak cladding temperature (K)**		**Uncertainty (K)**
	sample mean	95th percentile	$T_{95} - T_{mean}$
Blowdown			
regression	1137	1268	131
OSE	1140	1268	128
Reflood			
regression	1119	1228	109
OSE	1131	1245	114

3. APPLICATION OF CSAU TO SB LOCA

When the papers reviewing and comparing different methodologies [3, 28, 29] for code uncertainty assessment (four out of eight at that time proposed methods) were published, further studies on the national level were performed dealing with uncertainty evaluation. In the comparison of the methods it was shown [29] that only the CSAU method has no feature "continuous-valued output parameters". Further it was reported [28], that "no continuous-valued parameter was chosen in this[12] or any other case, indicating the inability to determine uncertainties for such parameters. Restriction to single-valued parameters, or only one or two of them, may oversimplify the problems and lead to wrong conclusions." In addition, a need for continuous-valued output parameters was also noted [30]. Therefore, the needs of the CSAU were identified first [31], the studies were performed and in answer to the needs the confirmatory application of the adapted CSAU to SB LOCA presented below was performed.

3.1. Preparation for the analysis

For the uncertainty quantification steps 1 through 13 of the CSAU method were performed[2]]. The RELAP5/MOD3.2 computer code was selected for uncertainty analysis consisting of adequate code documentation [32] required by CSAU method [2].

Selected scenario was SB LOCA with a 5.08 cm break in the cold leg at 50 s into the transient. Based on the careful examination of the transient and with the help of Nuclear Plant Analyzer (NPA) [33] the scenario was divided into 5 phases shown on Fig. 2. More detailed is scenario described in Ref. [34].

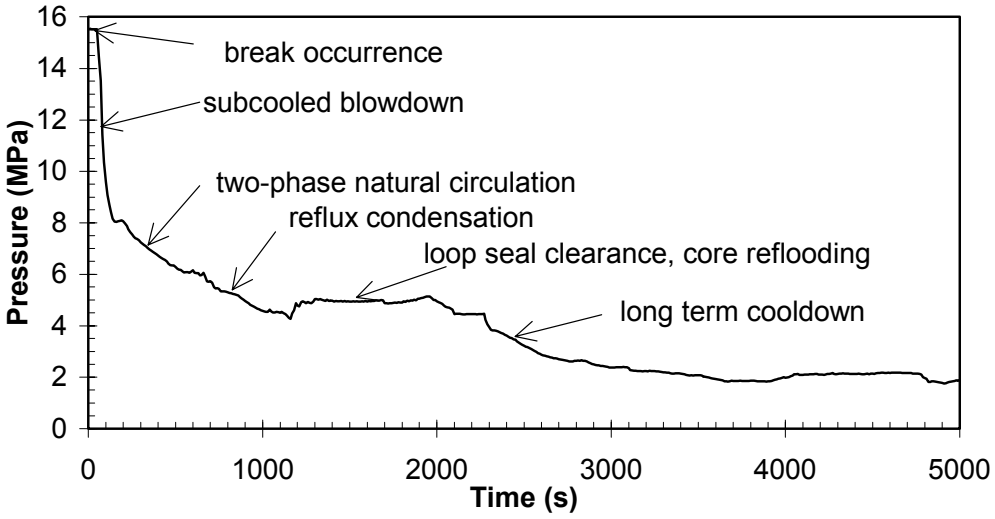


Figure 2. Subdivision of SB LOCA scenario into phases

Based on the phenomena identification and ranking process (PIRT) performed for SB LOCA in a two loop PWR (Krško NPP) as the most important were identified the following phenomena: heat transfer, critical flow, countercurrent liquid-vapour flow, liquid-vapour separation, decay heat, quench front propagation and interfacial friction.

The important parameters selected by PIRT were varied around nominal value in the range specified in Table 4 according to the given distribution. For these input uncertain parameters the ranges and their distributions were available from the previous SB LOCA

[12] i.e. SB LOCA analysis using CSAU [8] (comment of the authors of this paper).

study [8]]. The first safety parameter selected was peak cladding temperature (PCT). The second safety parameter was the "severity of the accident" S as was recommended and due to time constraints not used in the study described in Ref. [8]. The third single value parameter was the time when PCT occurs, t_{PCT}, as this time may vary from calculation to calculation. The parameter severity of the accident S is defined:

$$S = \int_0^{t_{rec}} \frac{\alpha_{core} H \cdot P}{P_0} dt \tag{1}$$

in which are α_{core} void fraction in the core, P the reactor power, P_0 initial reactor power, H the core height and t_{rec} time to recovery.

Table 4. Uncertainty ranges for selected parameters

Phenomenon	Code parameter	Distribution	Range	Bias	Mean value
heat transfer	heat transfer coefficient	uniform	±25%	-	1.0
critical flow	subcooled discharge coefficient	normal	±2 σ (σ=0.042)	0.083	0.917
	two phase discharge coefficient	normal	±2 σ (σ=0.062)	-0.435	1.435
countercurrent flow	-	N.A.	-	-	-
phase separation	interphase drag coefficient	normal	±2 σ (σ=0.0413)	-	1.0
decay heat	fission product yield factor	uniform	±10%	-	1.0

To reduce uncertainty due to nodalization standard input deck was used developed at Jožef Stefan Institute. To avoid the subjectivity [35], the standard input deck was qualified according to the procedure determined by the UMAE method [7]. These criteria were found very useful when standard nodalization is used for analysis (instead of the iterative step 8 of CSAU method).

3.2. Sensitivity and uncertainty analysis

In the sensitivity analysis total 59 calculations were performed. The calculated peak cladding temperatures for these calculations range from 975 K to 1233 K. The sensitivity calculations results were then used to build a response surface with regression models and OSE. The response surface was then used to simulate several thousands of cases in which the sensitivity parameters vary randomly according to their respective uncertainty range, distribution and bias (see Table 4). The uncertainty results for single valued safety parameters using OSE and the stepwise regression models were compared.

The results of comparison are shown in Table 5. First we can see that for PCT (same is true for S and t_{PCT}) in the case of OSE model used the maximum calculated value was the same as code calculated value. This is characteristic of OSE that between two code calculated values the function is monotonic. For regression models, for PCT and S the calculated values were lower and in the case of t_{PCT} the maximum value was higher than code calculated value, because for regression model the function between two neighbour points is not necessarily

monotonic. Second, the results showed that the value of coefficient of determination R^2 was very low for regression models. The reason for poor fit of regression model were complex and non-linear phenomena. The statistic R^2 was significantly improved when OSE was used instead of regression model.

Table 5. Probability statement for single parameter values for regression and OSE model

	peak cladding temperature, PCT (K)				**statistic**	
Model	5^{th} percentile value	mean value	95^{th} percentile value	maximum value	R^2	RMS
regression	1041.2	1079.3	1122.9	1173.6	0.416	-
OSE	1029.1	1085.3	1157.3	1233.0	0.972	1.55 K
	severity of accident, S (m s)				**statistic**	
	5^{th} percentile value	mean value	95^{th} percentile value	maximum value	R^2	RMS
regression	21.88	24.01	26.37	29.37	0.517	-
OSE	21.63	24.49	27.62	31.03	0.971	0.08 m s
	time of PCT occurrence, t_{PCT} (s)				**statistic**	
	5^{th} percentile value	mean value	95^{th} percentile value	maximum value	R^2	RMS
regression	1127.1	1221.9	1341.7	1579.8	0.880	-
OSE	1097.5	1215.8	1325.7	1412.0	0.996	1.06 s

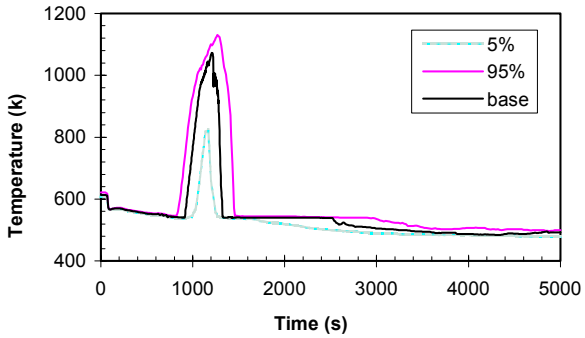


Figure 3. Lower and upper uncertainty bounds for cladding temperature.

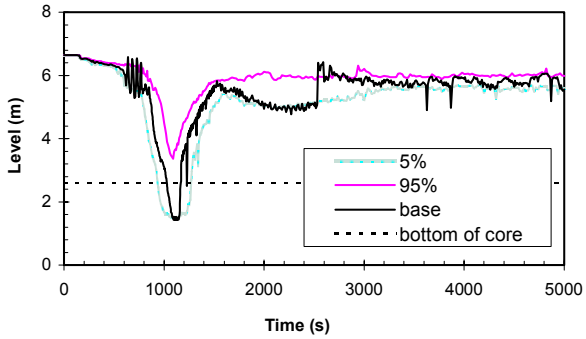


Figure 4. Lower and upper uncertainty bounds for core collapsed level.

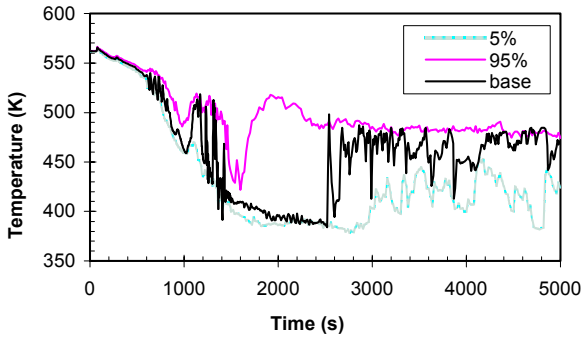


Figure 5. Lower and upper uncertainty bounds for core inlet temperature.

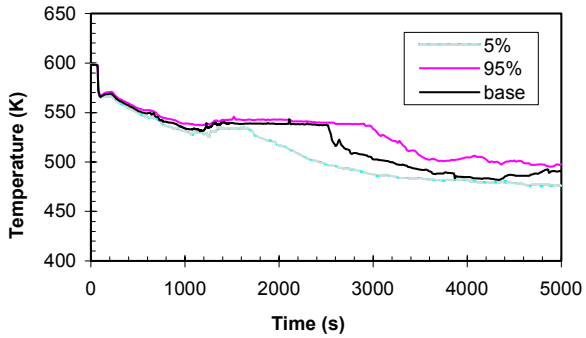


Figure 6. Lower and upper uncertainty bounds for core outlet temperature.

When comparing PCT to safety criteria the margin was sufficient. However, it should be noted that additional biases and uncertainties should be added not treated in the presented analysis, which would reduce the safety margin. Next, it was discovered that second safety parameter, severity of the accident S, was strongly correlated to peak cladding temperature with r=0.89 to be statistically significant. This means that severity of the accident could be used instead of PCT for safety parameters in scenarios in which PCT does not occur.

The major advantage of OSE is in its ability to automate uncertainty evaluation of single value or continues valued parameters while regression analysis needs to be performed to find the best fit. It is inherent to OSE to find the best fit from given information, i.e. optimal estimation. More code calculations provide more information for OSE to improve fit. This means that increased number of thermalhydraulic code calculations can increase confidence level of the results. This finding is common to GRS uncertainty method [6]. In Figs. 3 to 6 the lower and upper uncertainty bounds calculated by OSE for some safety and system parameters are shown. From Figs 3 and 4 it can be seen that uncertainties for PCT and core collapsed liquid level are related. The same is true for core inlet and core outlet temperature where after 1500 s both uncertainties increase. The number of output parameters for which uncertainty is determined is not limited.

4. CONCLUSIONS

In the paper applications of CSAU uncertainty method to LB and SB LOCA and contributions to the original CSAU are presented.

The best estimate analysis for LB LOCA was performed closely as possible following the CSAU methodology. The analysis demonstrated that the CSAU methodology can be applied to an individual plant. Since the analysis was built on the original one it was considerably less costly. For the analysis a fixed nodalisation was used. We relied on the well-tested standard input deck rather than using different nodalisations as an additional source of uncertainty. A new tool called OSE was adopted for response surface generation of PCT in LB LOCA calculation.

Due to complex and non-linear phenomena the best estimate plus uncertainty analysis of SB LOCA was prevented to be performed with regression analysis. Therefore the OSE was further improved. Advantages of OSE when compared to regression models were that OSE is not limited with complexity or non-linearity of the problem, the function is monotonic between neighbour points and achieved statistics is better in the case of OSE.

The applicability of the developed OSE tool was demonstrated for calculation of peak cladding temperature, severity of the accident and time of PCT occurrence and 9 important system and safety parameters during SB LOCA. The SB LOCA uncertainty analysis showed that safety margin for peak cladding temperature was sufficient when uncertainty of the order of 100 K was added to the mean value. However it should be noted that biases were not included in uncertainty analysis and have to be added separately to make the analysis complete.

The findings of the study suggest that OSE can be used for response surface generation of any safety or system parameter in the thermal-hydraulic safety analyses with uncertainty evaluation.

REFERENCES

[1] BOYACK, B., DUFFEY, R., GRIFFITH, P., LELLOUCHE, G., LEVY, S., ROHATGI, U., WILSON, G., WULFF, W., AND ZUBER, N., "Quantifying Reactor Safety Margins, Application of Code Scaling, Applicability, and Uncertainty Evaluation Methodology to a Large-Break, Loss-of-Coolant Accident", NUREG/CR-5249, US Nuclear Regulatory Commission (1989).

[2] TECHNICAL PROGRAM GROUP: BOYACK, B. E., CATTON, I., DUFFEY, R. B., GRIFFITH, P., KATSMA, K. R., LELLOUCHE, G. S., LEVY, S., ROHATGI, U. S., WILSON, G. E., WULFF, W., AND ZUBER, N.,"Quantifying Reactor Safety Margin, Parts 1 to 6", J. Nucl. Eng. Des., 119, p.1 (1990).

[3] GLAESER, H., POCHARD, R., "Review on Uncertainty Methods for Thermal Hydraulic Computer Codes", Proc. Int. Conf. New Trends in Nuclear System Thermalhydraulics, Pisa, Italy, May 30–June 2, Vol. 1, p. 447 (1994).

[4] REOCREUX, M., "Safety Analysis and Best Estimate codes", Proc. 4th Mtg.: Nuclear Energy in Central Europe, Bled, Slovenia, September 7–10, p.9, Nuclear Society of Slovenia (1997).

[5] QUINSY, A., BRUN, B., DE CRÉCY, F., "The adjoint sensitivity method, a contribution to the code uncertainty evaluation", J. Nucl. Eng. Des., 149, p.357 (1994).

[6] GLAESER, H., HOFER, E., CHONJACKI, E., QUNSY, A., RENAULT, C., "Mathematical techniques for uncertainty and sensitivity analysis", Proc. Validation of Systems Transients Analysis Codes, FED-Vol. 223, Hilton Head, South Carolina, August 13–18, p. 75, American Society of Mechanical Engineers (1995).

[7] D'AURIA, F., DEBRECIN, N., GALASSI, G. M., "Outline of the Uncertainty Methodology Based on Accuracy Extrapolation", Nucl. Technol., 109, p.21 (1995).

[8] 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", NUREG/CR-5818, EGG-2665, Idaho National Engineering Laboratory (1992).

[9] GLAESER, H., "Validation and Uncertainty Analysis of the ATHLET thermal-hydraulic computer code", Proc. 2nd Regional Mtg.: Nuclear Energy in Central Europe, Portorož, Slovenia, September 11-14, p.591, Nuclear Society of Slovenia (1995).

[10] PARK, S. R., BAEK, W. P., CHANG, S. H., LEE, B. H., "Development of an uncertainty quantification method of the best estimate large LOCA analysis", J. Nucl. Eng. Des., 135, p.367 (1992).

[11] MAVKO, B., STRITAR, A., PROŠEK, A., "Application of Code Scaling, Applicability and Uncertainty Methodology to Large Break LOCA Analysis of Two-Loop PWR", J. Nucl. Eng. Des., 143, pp. 95-119 (1993).

[12] HASKIN, E.F., BEVAN, B. D., DING,C., "Efficient uncertainty analyses using fast probability integration", J. Nucl. Eng. Des., 166, 225 (1996).

[13] .YEUNG, W. S,. HARVEY, R. C, SHIRKOV, J.,. SUNDARAM, R. K, SARDY S., "Application of the CSAU methodology to BETHSY SBLOCA test 9.1b using RELAP5/MOD3.1", presented at RELAP5 International Users Seminar, Dallas, Texas, March 17-21, 1996.

[14] GLAESER, H., WICKETT, T., CHONJACKI, E., D'AURIA, F. AND PEREZ, C., "OECD/CSNI Uncertainty Methods Study for "Best Estimate" Analysis", Proc. Int. Mtg. Best-Estimate Methods in Nuclear Installation Safety Analysis (BE-2000), Washington, DC, November (2000).

[15] YOUNG, M.Y., BAJOREK, S.M., NISSLEY, M.E., NGUYEN, S.B., Best estimate analysis of the large break loss of coolant accident, Proc. of ICONE6, American Society of Mechanical Engineers, Japan Society of Mechanical Engineers and Societe Francaise D'Energie Nucleaire, pp. 1-19 of ICONE6-6252 (1996).
[16] TAKEUCHI. K. AND NISSLEY M.E., "Best Estimate Loss-of-Coolant Accident Licensing Methodology Based on WCOBRA/TRAC Code", Proc. Int. Mtg. Best-Estimate Methods in Nuclear Installation Safety Analysis (BE-2000), Washington, DC, November (2000).
[17] KAWAMURA S. AND HARA T., "Best estimate Methods for Licensing Analysis", Proc. Int. Mtg. Best-Estimate Methods in Nuclear Installation Safety Analysis (BE-2000), Washington, DC, November (2000).
[18] STRITAR, A., MAVKO B., PROŠEK, A., "The Best Estimate Analysis of Large Break Loss of Coolant Accident with Uncertainty Evaluation", Transactions of the American Nuclear Society, Vol.66, pp.: 584-585, Chicago (1992).
[19] PROŠEK, A., MAVKO, B., "Evaluating Code Uncertainty — I: Using the CSAU Method for Uncertainty Analysis of a Two-loop PWR SBLOCA", Nuclear Technology, 126, pp. 170-185 (1999).
[20] PROŠEK, A., MAVKO, B., "Evaluating code uncertainty-II: An optimal statistical estimator method to evaluate the uncertainties of calculated time trends", Nuclear Technology, 126, pp. 186-195 (1999).
[21] RANSOM, VICTOR H., et al., "RELAP5/MOD2 Code Manual, Vol. 1, Vol. 2, Vol. 3", NUREG/CR-4312, EGG-2396, Rev.1, Idaho (March 1987).
[22] RELAP5/MOD2 MODELS AND CORRELATIONS, Dec. 1987 (DRAFT)
[23] PETELIN, S., GORTNAR, O., MAVKO, B., "RELAP5/MOD2 Split Reactor Vessel Model", San Francisco: American nuclear society, Nov. 10-14, 1994, 64, pp. 686-688 (1994).
[24] PETELIN, S., MAVKO, B., GORTNAR, O., "Analysis of a Nuclear Plant Transient Caused by a Stuck Spray Valve", Kerntechnik, Vol. 56, 5, pp. 300-306 (1991).
[25] PARZER, I., PETELIN, S., MAVKO, B., "Feed&Bleed Procedure Mitigating the Consequences of a Steam Generator Tube Rupture Accident", Proc. Annual Meeting on Nuclear Technology, 5.-7.5.1992, Karlsruhe, pp.: 131-134 (1992).
[26] STRITAR, A., MAVKO, B., "Influence of Steam Generator Plugging and Break Size on Large Break Loss-of-Coolant Accidents", Nuclear Safety, 32, 3, pp.: 363-374 (1991).
[27] PROŠEK A., MAVKO B., STRITAR, A., "Statistical method used for LB LOCA PCT calculation", Proc. Nuclear Energy in Central Europe: Present and Perspectives, Nuclear Society of Slovenia (1993).
[28] HOLMSTRÖM, H., GLAESER, H., WICKETT, A., WILSON, G., "Status of Code Uncertainty Evaluation Methodologies", Proc. Int. Conf. on New Trends in Nuclear System Thermalhydraulics, Pisa, Italy, May 30–June 2,Vol. 1, p.437, ETS (1994).
[29] D'AURIA, F., LEONARDI, M., GLAESER, H., AND POCHARD, R., "Current status of methodologies evaluating the uncertainty in the prediction of thermal-hydraulic phenomena in nuclear reactors", Proc. Two-Phase Flow Modeling and Experimentation 1995, Roma, Italy, October 9-11, p.501, ETS (1995).
[30] HOLMSTRÖM, H., TOUMISTO, H., "Applicability of the CSAU methodology to safety assessments", J. Nucl. Eng. Des., 132, p. 415 (1992).
[31] PROŠEK, A., MAVKO, B., "Needs of the CSAU Uncertainty Method", Proc. Nuclear Option in Countries with Small and Medium Electricity Grids, Dubrovnik, Croatia, Croatian Nuclear Society; (2000).
[32] RELAP5 CODE DEVELOPMENT TEAM, "RELAP5/MOD3 Code Manual, Vols. 1 to 7", NUREG/CR-5535 (1995).

[33] SNIDER D.M., WAGNER, K.L, GRUSH, W.H, JONES, K.R., "Nuclear Plant Analyzer", NUREG/CR-6291, INEL-94/0123, Vols. 1 to 4, Idaho National Engineering Laboratory (1995).
[34] KLJENAK, I., PROŠEK, A., "Development of a Phenomena Identification and Ranking Table for a Small-Break Loss of Coolant Accident scenario", Proc. 4th Regional meeting: Nuclear Energy in Central Europe, September 7-10, 1997, Bled, Slovenia, Nuclear Society of Slovenia (1997).
[35] AKSAN, S.N., D'AURIA, F., STÄDTKE, H., "User effects on the thermal-hydraulic transient system code calculations", Nuclear Engineering and Design, 145, 159-174 (1993).

SAFETY MARGINS OF RBMK-1500 ACCIDENT LOCALISATION SYSTEM AT IGNALINA NPP

S. RIMKEVIČIUS, E. URBONAVIČIUS, B. ČĖSNA
Lithuanian Energy Institute, Laboratory of Nuclear Installation Safety,
Kaunas, Lithuania

Abstract. Accident localisation system (ALS) at Ignalina NPP forms the last barrier against release of radioactive material to environment. According to functional principle the ALS could be attributed to so called "pressure suppression" type containment. It means, that ALS uses condensing pools, which condense the released steam in order to reduce the peak pressures that can be reached during any loss of coolant accident. The main safety function for ALS is to contain the radioactive materials released in the course of accident and to limit the releases within specified limits. The ALS performance during the accidents relies upon the ALS structure capability to withstand the loads. The maximal pressure, which can be reached during accident, is one of the most important parameters, defining ALS capability to remain intact and to perform its safety function. The maximal loads on ALS could be reached during the maximum design basis accident (MDBA). The MDBA is defined as the guillotine (i.e. complete) rupture of the pressure header of the main circulation pumps. The pressure header is a sizable element of the RBMK-1500 piping: the length of this component is ~18.5 m, the inner diameter is 900 mm. Other important design basis event is the break of a Group Distribution Header (GDH). This break represents a medium size LOCA (internal diameter of GDH — 0.295 m), but it is important from the point of view of ALS performance, because GDH piping is located in a restricted space below the reactor core. The GDHs are fed from the pressure header and distribute coolant to fuel channels. There are 20 GDH units in a circulation loop, or a total of 40 in the plant.The behaviour of main thermal hydraulic parameters in ALS is presented in this paper for both of these LOCAs (MDBA and GDH break). The release rates through the breaks were calculated by applying the RELAP5 code. A number of calculations variants were performed in order to evaluate ALS response to MDBA as well as to GDH break. The different calculation codes (CONTAIN, RALOC) and different boundary conditions regarding water droplets behaviour in the compartments were used in these calculations. The maximal calculated pressures in ALS compartments are below the maximum allowed design pressures for both presented LOCA even in the case of most conservative boundary conditions. The maximal values of pressure and temperature calculated in ALS compartments are compared with design values of corresponding parameters and the safety margins are defined.

1 INTRODUCTION

The RBMK-1500 is graphite moderated, boiling water, channel type reactor with a total of 1661 vertical parallel fuel channels and numerous components such as headers, pumps, valves etc. The RBMK-1500 reactors of the Ignalina NPP are protected by a pressure suppression type containment, which, because of its specialized nature, is referred to as the Accident Localisation System. The ALS forms the last barrier against release of radioactive material to environment.

Two limiting loss-of-coolant accidents are presented briefly in this paper:

- Maximum design basis accident — i.e. rupture of MCP pressure header in reinforced leaktight compartments of ALS
- Group distribution header rupture in lower water piping compartment of ALS

The ALS models for the CONTAIN 11AF [1], [2] and RALOC4 [3] codes are presented and calculation results are discussed in this paper. Safety margins are defined for different zones of ALS.

2. SHORT DESCRIPTION OF IGNALINA NPP ACCIDENT LOCALIZATION SYSTEM

A schematic representation of the Ignalina NPP building including the relative location of the ALS system components is shown in Figure 1. The reactor core is shown in the middle of the figure, the regions, which constitute the ALS are included within the heavy outline. Most of MCC piping (MCP suction (3) and pressure (4) headers, GDH (5), the piping leading to the core) and major components (pumps (2), valves) are located within the ALS, which consists of a series of reinforced enclosures. Pressure buildup within the compartments in the event of LOCA is mitigated by a unique ALS design

The ALS consists of the following major parts (Figure 9):

- reinforced leaktight compartments I and II
- leaktight compartments III and IV
- ALS towers (compartment V-X)
- condensing tray cooling system (8).

The ALS is served by two 'towers', which house five, vertically positioned condensation trays. The condensation trays are divided into two sets:

- The lower four trays, which contain most of the condensing pool water and are intended to mitigate the consequences of breaks of the components and piping located in ALS leaktight compartments (compartments I, III and IV in Figure 1);
- The upper tray in each tower (tray 5) is a separate unit, which receives the steam from the set of steam relief valves. The 5-th tray in the left tower is also designed to receive the releases in the case of fuel channel rupture in reactor core.

In the case of LOCA in ALS the CTCS is activated by high temperatures (35^{o}C) of water in lower four condensing trays or by an activation signal of ECCS. The cooled water is directed simultaneously to the four bottom condensing pools and sprays of gas holding chambers. The valves on the water supply lines open automatically.

Generic description of the ALS is provided in the Source book of the Ignalina NPP [4] and Ignalina NPP SAR [5].

3. DESCRIPTION OF ALS MODELS EMPLOYED FOR ANALYSIS

3.1. ALS model for code CONTAIN

The CONTAIN code was employed for the simulation of the Accident Localisation System response to the LOCA in ALS compartments. The 23 node nominal model for the Ignalina ALS was developed Figure 2 for calculations employing CONTAIN code. This model is suitable for analyzing breaks in the major piping components. The break in the case of MDBA was assumed in the cell #5, and in the case of GDH break — in the cell #20. For the analysis of the PH break, the model is reduced to 20 nodes, as 3 compartments, located in restricted space below the reactor core (cells #20, #21 and #22), are not affected. The water inventory of the four lower trays is combined and is represented by one equivalent pool in each ALS tower (cells #1 and #2). The model includes provisions for timed venting of non-condensable gases and for overflow of water from pools.

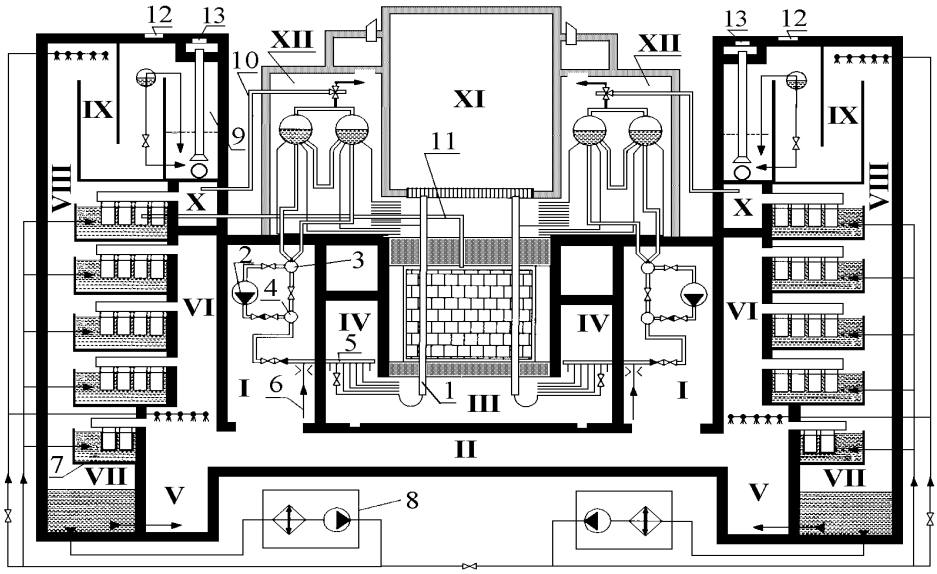


Figure 1. Principal ALS schematic.

1 – FC, 2 – MCP, 3 – SH, 4 – PH, 5 – GDH, 6 – ECCS header, 7 – condensing trays (pools), 8 – Condenser Tray Cooling System, 9 – air discharge pipe section, 10 – MSV steam discharge pipe, 11 -RCVS piping from reactor cavity, 12 – blow-out panels, 13 – tip-up hatches
Compartments: *I – reinforced compartments enclosing the major primary system components (MCP, SH, PH and downcomers), II – reinforced steam removal corridor, III- under-reactor compartment, IV – compartments of GDH and lower water piping, V – BSRC, VI – vertical shafts of ALS tower, VII – HCC, VIII – air venting channel, IX – gas holding chamber, X – top steam reception chamber, XI- reactor hall, XII – compartments of drum separators*

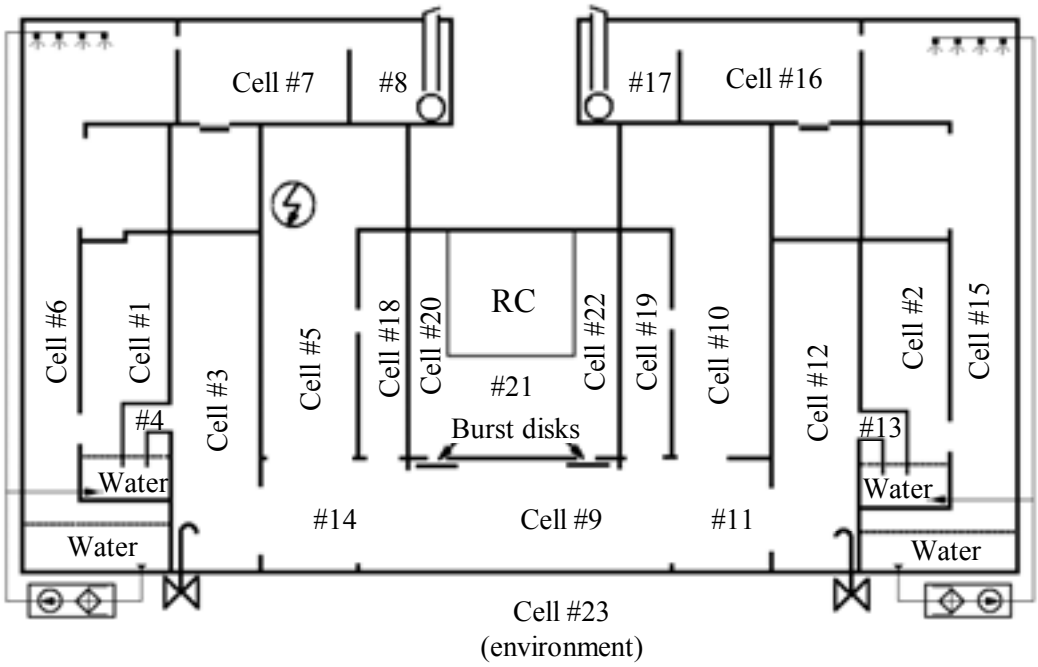


Figure 2. The nodalization scheme of the ALS model for the code CONTAIN.

In the case of steam-gas mixture flow to the condensing pools the water level there increases due to pool swelling (this phenomena is characteristic in the initial phase of the accident when the high amount of non-condensable gas flows to pools) and steam condensation. If the water level in the condensing pools reaches 1.1 m the overflow to HCC occurs. Excess water from these pools spills over into the HCC, this pool serves as the principal source of water for the CTCS and ECCS (ECCS is not included in ALS model for code CONTAIN).

The air release from the ALS towers (from cell #8 and #17) to the environment was simulated employing special junctions that according to design close in 5 min after the accident start.

The CTCS operation was considered in the performed calculations by the simulation of pumps and heat exchangers. The CTCS assumed to supply the water to the four bottom condensing pools and upper sprays. The water flow to each tower of ALS is 2500 m^3/h.

The description of the heat exchange with the structures of the ALS depending on the location of the structure is presented in [6].

3.2. Main differences in ALS models for CONTAIN and RALOC

The balance between energy sources and sinks determines the thermalhydraulic behavior of ALS in the case of LOCA. Besides energy release from the break the following energy sources and sinks are important under LOCA conditions:

1. Heat flux to/from the structures;
2. Condenser Tray Cooling System;
3. “Clean air” venting system;
4. Emergency Core Cooling System;
5. Water drainage systems;
6. ALS make-up system (for water supply to hot condensate chamber).

Only the first three energy source/sinks mechanisms were considered in the analysis performed employing CONTAIN code. The simulation of drainage, ALS make-up and ECCS systems is rather complicated in CONTAIN code because of specific algorithm of these systems activation/deactivation.
All main technical systems connected to ALS are taken into account and modelled in detail employing RALOC4 code in order to consider all the energy sources and sinks. The analysis of the ALS behaviour in case of a GDH break employing code RALOC4 was performed using a 26 node model with 84 junctions of different type (including 10 pump systems) and 89 structures (heat slabs). The nodalisation scheme is presented in Figure 3, where the linkage of the CTCS, ECCS, make-up system and drainage pumps is pictured.

The simulation of "clean air" venting system in ALS model for RALOC4 code is more realistic as well in comparison with model for CONTAIN code, because of proper simulation of knock-out hatches installed in the ceiling of the ALS towers. The knock-out hatches were modeled as flaps available in RALOC4 code. It allows to consider inertia of flaps motion and their partially opening depending on pressure difference.

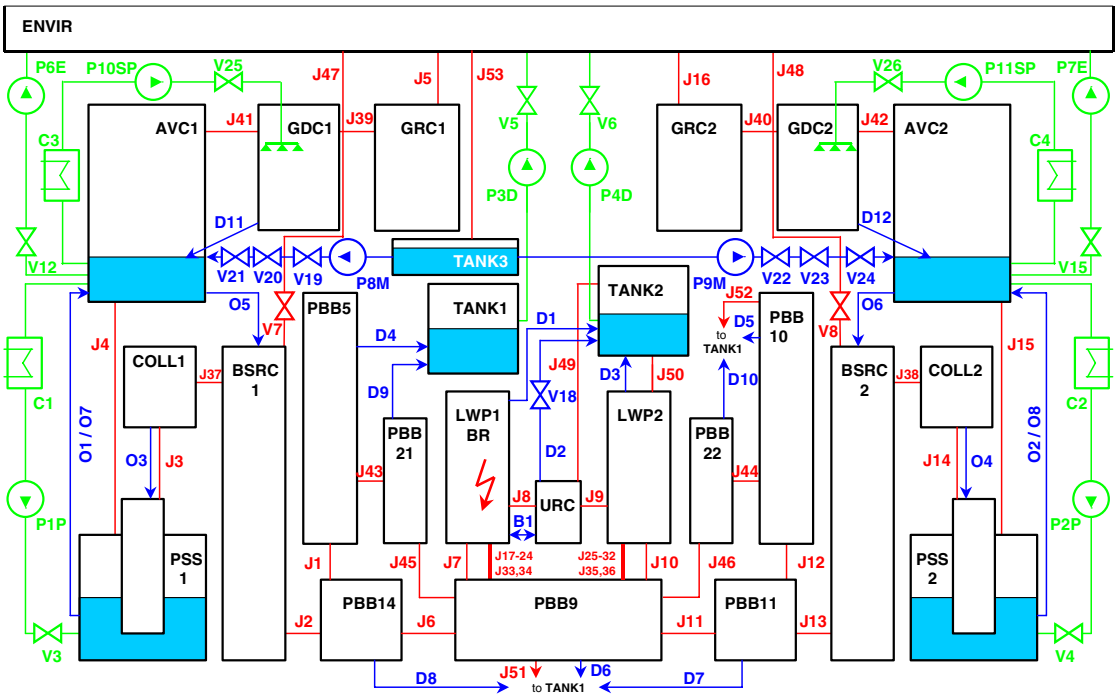


Figure 3. Ignalina NPP ALS model for RALOC4 code.

4. CALCULATION RESULTS IN THE CASE OF MDBA

4.1. Contain results

The calculations were performed using the RELAP5 source function. The PH break analysis is carried out for the Ignalina NPP Unit 2 with the effect of by-pass leakage. Unit 2 was chosen for analysis because the ALS of this unit has smaller leakage area than the ALS of Unit 1. Therefore, smaller amount of mass and energy can be released to environment from Unit 2 causing more severe thermal hydraulic conditions inside the ALS compartments.

The calculations were performed for two bounding assumptions regarding behaviour of liquid fraction of the break flow:

- all liquid fraction of the break flow remains suspended (without ‘dropout’ option in calculations)
- all liquid fraction of the break flow is removed from the atmosphere and it is placed in the sump (using ‘dropout’)

Figures 4 and Figure 5 present the results of CONTAIN calculations for the most conservative case regarding the behavior of liquid fraction of the break — i.e. when all liquid fraction of the break flow remains suspended.

Figure 4 shows the peak pressure of the break and neighboring compartments (see cell #5 and #18 in Figure 2) itself, the brief spike generated in the compartments (cell #3) just in front of the condensation trays by the inertia of the water, and the pressure in the compartments behind the condensation trays (cells #1, #6 and #8). The pressure difference between the compartments before the condensation trays and those beyond was produced by the static head of the water in the condensation trays.

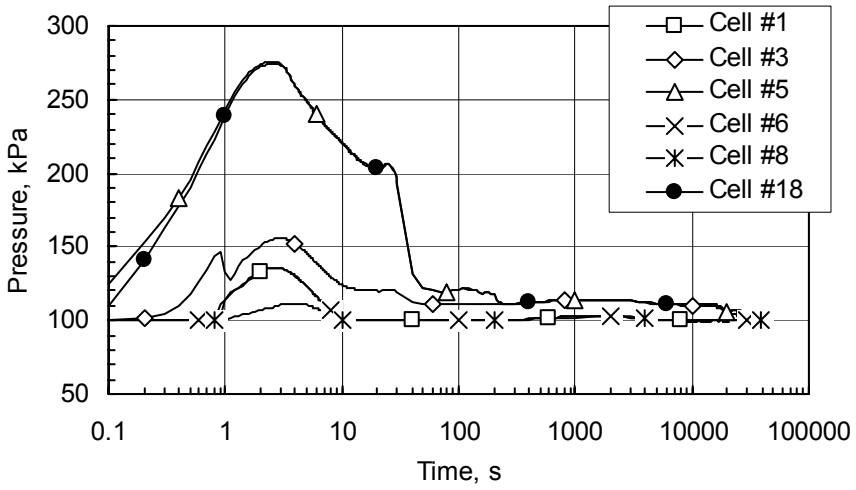


Figure 4. MDBA. The pressure behaviour in the ALS.

The pressure peaks in right side ALS compartments are lower (not presented in this paper), because PH break is assumed to occur in the left side ALS compartment.

The atmospheric temperatures in the main compartments of both ALS sides are shown in Figure 5. The temperatures show that the atmosphere of the compartments before the condensing pools (cells #5, #18 and #3) was maintained at saturation temperature for the long term. The compartments beyond the condensation trays (cells #1, #6 and #8) do not reach saturation temperature.

The maximal calculated temperatures in reinforced leaktight compartments of ALS in the case of maximum design basis accident are below the design temperature (143^{o}C).

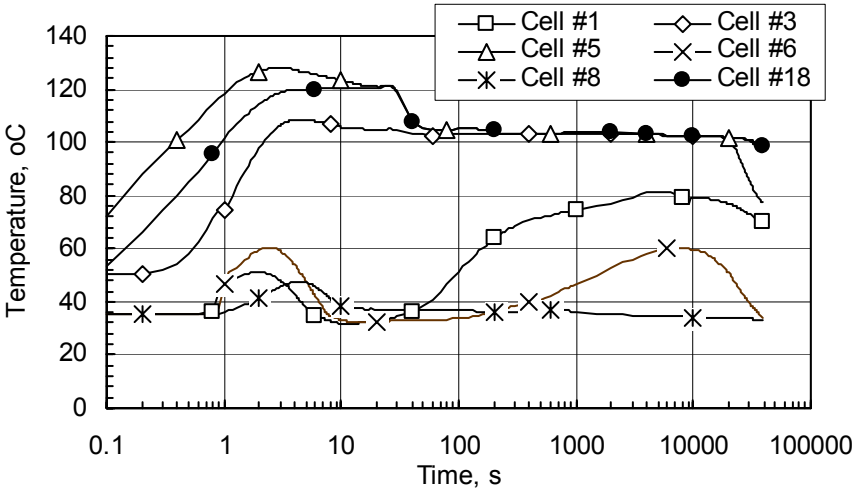


Figure 5 MDBA. The temperature behaviour in the ALS.

4.2. Comparison of different calculation cases

Code-to-code comparison performed for the analysis of MCP pressure header rupture employing codes CONTAIN and RALOC. Figure 6 and Figure 7 present the influence of the water carryover coefficient on the pressure and comparison of results obtained by codes CONTAIN and RALOC4.

In Figure 7 there are compared the CONTAIN results calculated at boundary conditions (with and without 'dropout') with the RALOC4 code results assuming that 40% of water suspended in the compartments atmosphere is carried with atmospheric flow (water carryover coefficient PHID=0.4). Further on the flow path this coefficient is gradually decreased to zero.

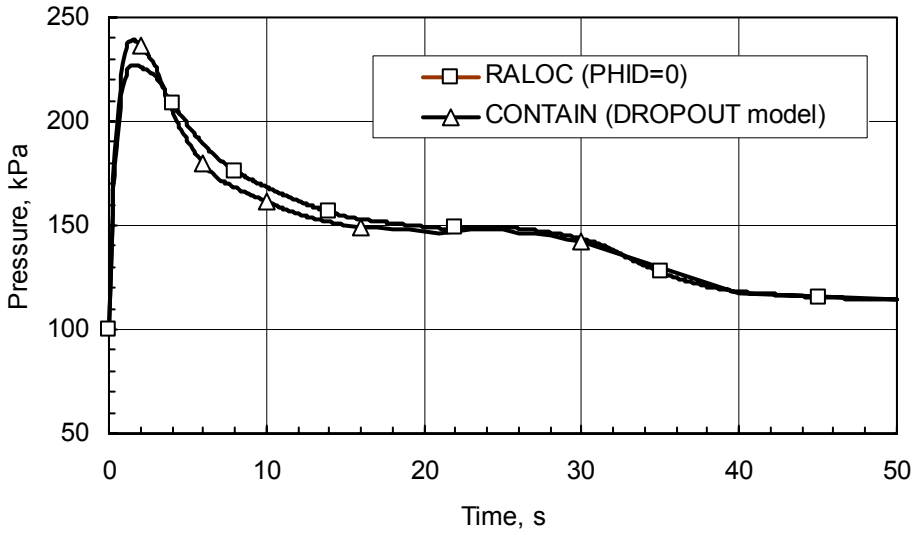


Figure 6. Comparison of the calculated pressure in accident compartment employing codes CONTAIN and RALOC4 without consideration of water droplets carryover.

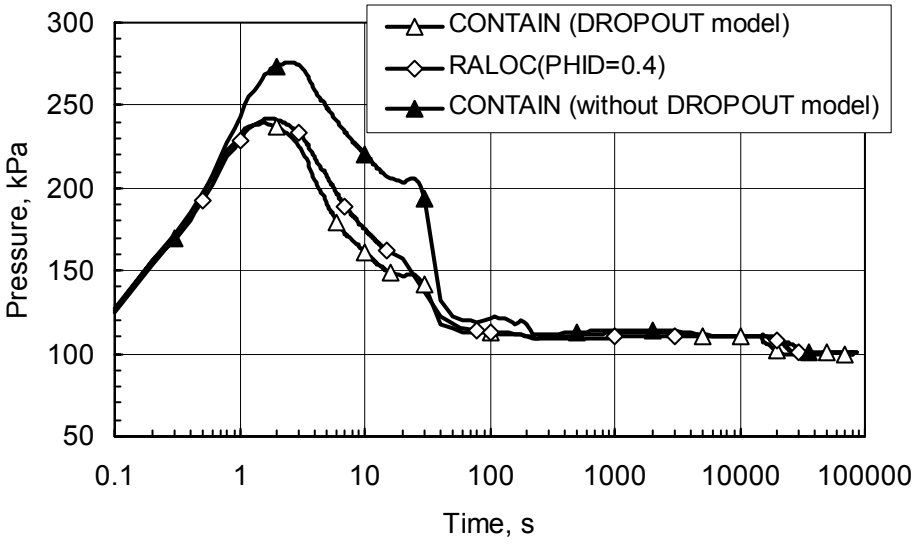


Figure 7. Pressure header rupture. Pressure in the accident compartment.

5. CALCULATION RESULTS IN THE CASE OF GDH BREAK

5.1. RALOC4 results

The ALS buildings structures are assumed fully leaktight for GDH break analysis — i.e. no structural leakage (i.e. zero leakage) to the environment. This assumption is conservative regarding thermal hydraulic parameters, because one of energy removal mechanisms is neglected and it leads to higher calculated values of pressure and temperature in ALS.

The Figure 8 shows the peak pressure in the LWP and URC compartments, the brief spikes of pressure generated in the reinforced leaktight compartments (see node PBB9 in Figure 11), and in left ALS tower before condensing pools water layer (node BSRC) and behind it (nodes PSS1 and GDC1). These nodes practically represent pressure behavior in all compartments of ALS.

Pressure behaviour is resulting from following factors:

- opening of rupture discs from LWP compartments to the steam distribution corridor PBB9 of reinforced leaktight compartments (4 flaps and 15 rupture discs are opened out of 18)
- closure of the release of clean air into the environment via the junctions J5 and J16 after 300 s
- different air concentration in the compartments before and behind condensing pools (this feature has influence on pressure behaviour after 11000 s of accident)

The maximum pressures calculated for the ALS compartments are well below the design pressure values (80 kPa gauge for LWP and URC as well as for ALS tower).

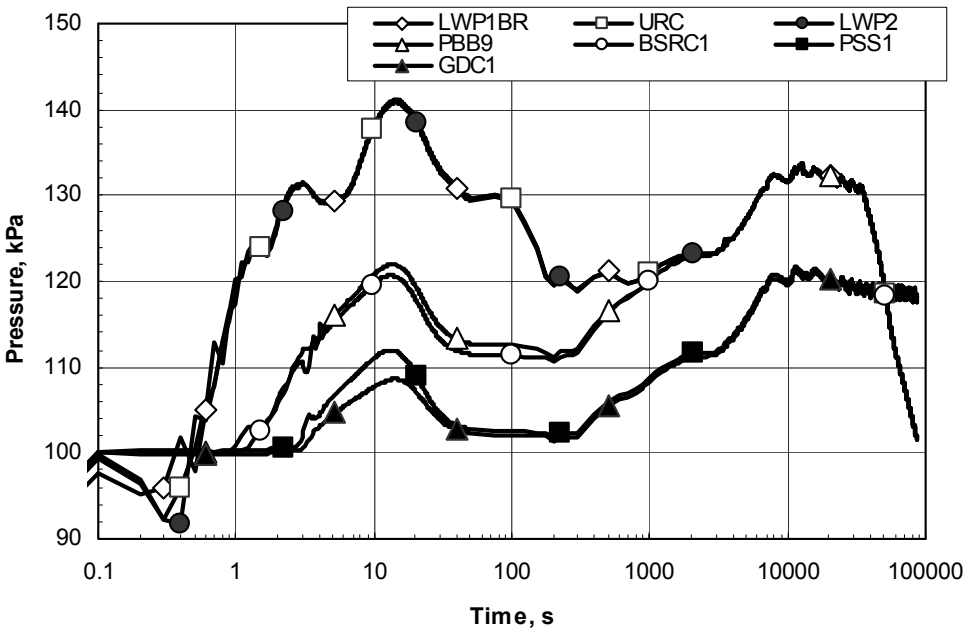


Figure 8. GDH break. Pressure behaviour in ALS compartments.

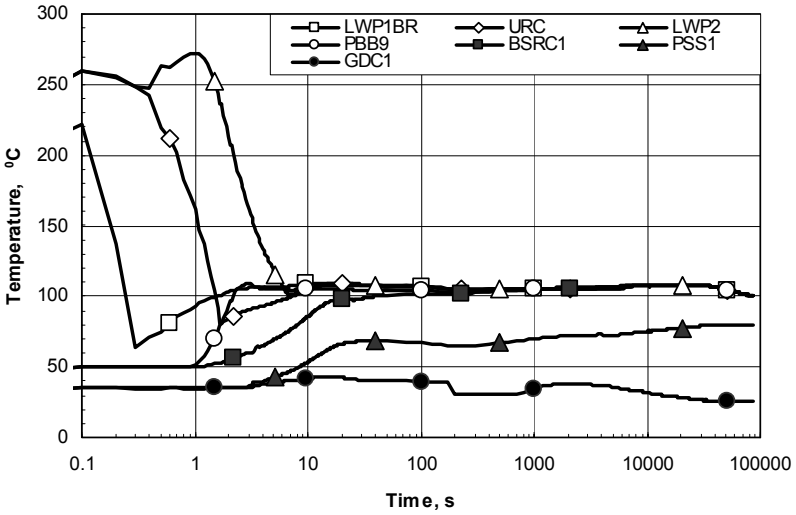


Figure 9. GDH break. Temperature behaviour in ALS compartments.

The log scale plot in Figure 9 emphasizes the high initial temperatures present in the regions below the core where the break takes place. Temperature histories for LWP and URC nodes show that the high initial temperature (260 °C) in the compartments below the reactor decreases down to saturation temperature during the first 10 s of the LOCA. In the compartments beyond condensing trays saturation temperatures are not reached (Figure 9). There is no risk regarding exceeding of temperature design limits, because temperature in accident compartments (LWP and URC nodes) is decreasing after accident initiation, and temperatures in other ALS zones are lower than in the case of MDBA.

5.2. Comparison of different calculation variants results

The comparison of results, calculated by codes RALOC4 and CONTAIN in the case of GDH break, shows, that the tendencies of pressure behaviour are similar, but absolute values differ (Figure 10). This difference is caused by more realistic treatment of energy sinks and water behaviour in calculations performed employing RALOC4 code.

6. ALS SAFETY MARGINS

The design pressures in ALS compartments are indicated in Figure 11. The reinforced leaktight compartments are designed for the pressure of 400 kPa. The pressure is decreasing by the coolant path and in bottom steam reception chamber the design pressure is 200 kPa. The pressure behind condensing pools decreases down to 180 kPa.

As it is seen in Table 1, the maximal calculated pressures in ALS compartments in the case of MDBA and in the case of GDH rupture are below the maximum allowed design pressures even in the case of most conservative boundary conditions. The interval of maximal calculated pressures, specified in the Table 1, covers the range of pressures, received using different boundary conditions and includes results obtained by both codes — CONTAIN and RALOC4. The safety margin for overpressure in ALS compartments is calculated using upper value from the range of maximal calculated pressures. The maximal calculated pressures in reinforced leaktight compartments and in ALS tower are taken from MDBA analysis, because they exceed the pressures, which could be reached in the case of any other design basis accidents. The maximal calculated pressures in lower water piping compartment is taken from GDH (i.e. largest pipe in this ALS zone) break analysis.

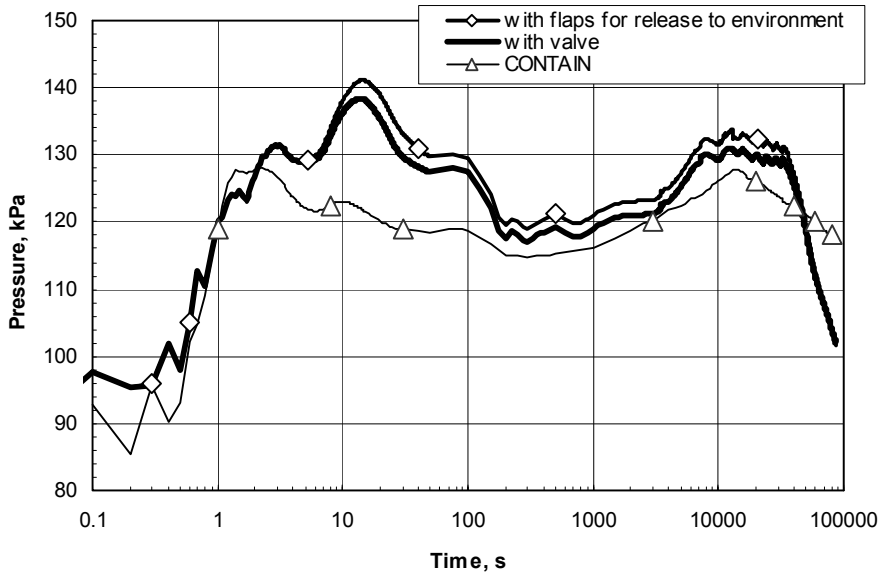
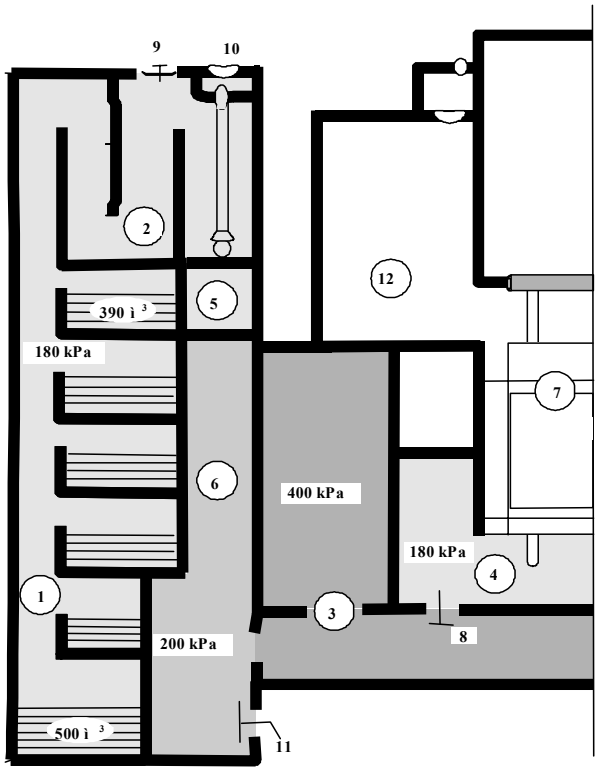


Figure 10. Comparison of pressure in break room calculated by RALOC4 and CONTAIN codes.



1	Air venting channel	7	Reactor cavity
2	Gas holding chamber	8	Steam relief valve
3	Reinforced leaktight compartments	9	Blow-out panels
4	Lower water piping compartment	10	Tip-up panels
5	Top steam reception chamber	11	Vacuum breakers
6	Bottom steam reception chamber and steam distribution corridor	12	Drum separator compartment

Figure 11. Design pressures in ALS compartments.

Table 1. ALS safety margins

ALS compartments group	Design pressure, kPa	Maximal calculated pressure, kPa	Safety margin	
			kPa	%
Reinforced leaktight compartments	400	227-276	124	41
ALS tower before condensing pools	200	156-163	37	37
ALS tower behind condensing pools	180	136-150	30	37
Lower water piping compartment	180	128-141	39	49

The analysis showed, that allowed temperature limits in ALS compartments potentially could be reached only in reinforced leaktight ALS compartments during MDBA. The maximal calculated temperatures in this case are in the range of 126-134^{o}C. This interval covers the temperatures, received using different boundary conditions and includes results obtained by both codes — CONTAIN and RALOC4. Thus, there is at least 9^{o}C (6%) safety margin to design temperature (143^{o}C).

7. CONCLUSIONS

1. The maximal calculated pressures and temperatures in ALS compartments in the case of maximum design basis accident and in the case of group distribution header rupture are below the maximum allowed corresponding parameters even in the case of most conservative boundary conditions.
2. Depending on the modelling of the water behaviour in the atmosphere the maximum calculated overpressure in ALS reinforced leaktight compartments may vary from 127 kPa to 176 kPa in the case of MDBA. The safety margin for the pressure in the case of MDBA for ALS reinforced leaktight compartments and ALS towers is about 40%.
3. Depending on the modelling of the water behaviour in the atmosphere the maximum calculated overpressure in lower water piping compartment of ALS may vary from 28 kPa to 41 kPa in the case of group distribution header rupture. The safety margin for the pressure in the case of group distribution header rupture reaches almost 50%.

REFERENCES

[1] MURATA, K. K., et al., Reference Manual for the CONTAIN 1.1: Code for Containment Severe Accident Analysis, NUREG/CR-5715 (1991).

[2] MURATA, K. K., Change document for update C11af: CONTAIN 1.2 pre-release bugfixes (1995).

[3] KLEIN-HESSLING W., et al., RALOC/MOD4.0 User Manual, Gesselschaft fur anlagen- und Reaktorsicherheit (GRS) mbH (1995).
ALMENAS, K., KALIATKA, A., UŠPURAS, E., Ignalina RBMK-1500. A source book, Extended and updated version, Kaunas (1998).

[4] Ignalina Safety Analysis Report, 1996. Vol.1.

[5] RIMKEVIČIUS, S., ČĖSNA, B., Simulation of the Accident Localisation System at Ignalina NPP using the DRASYS code in the case of Group Distribution Header rupture, Energetika, 1997, No. 2, P. 49-56 (In Russian).

NOMENCLATURE

ALS	Accident Localisation System
BSRC	Bottom Steam Reception Chamber
CTCS	Condenser Tray Cooling System
ECCS	Emergency Core Cooling System
FC	Fuel Channel
GDH	Group Distribution Header
HCC	Hot Condensate Chamber
LOCA	Loss of Coolant Accident
LWP	Lower Water Piping
MCC	Main Circulation Circuit
MCP	Main Circulation Pump
MDBA	Maximum Design Basic Accident
MSV	Main Safety Valve
NPP	Nuclear Power Plant
PH	Pressure Header
RBMK	Russian Acronym For ‘Large Power Channel Reactor’
RCVS	Reactor Cavity Venting System
SAR	Safety Analysis Report
SH	Suction Header
URC	Under Reactor Compartment

ANALYSIS OF LOCA D=200 mm FOR NPP KOZLODUY UNITS 3&4 WITH RELAP5/Mod3.2 AND CATHARE CODES. EVALUATION OF THE RESULTS UNCERTAINTY

I. STANEV
Energoproekt plc,
Bulgaria

F. D'AURIA
University of Pisa,
Italy

Abstract. Since 1993 NPP Kozloduy is performing an extensive program for upgrading of the safety level of units 3 and 4 (WWER-440/230) according to the current international standards. One important part of this program is the qualification of the units for a Large Break LOCA (200 mm diameter) Design Basis Accident. The first step is a set of conservative analyses of the core cooling margins with the RELAP5/Mod.3 code, performed by Energoproekt plc. Then a team from the University of Pisa, supported by Energoproekt experts, performed a best estimate analysis with an independently developed input deck, followed by an uncertainty evaluation study. Finally, a CATHARE calculation is performed in order to evaluate and avoid code-specific influence on the results. The main conclusion is that the NPP Kozloduy units 3 and 4 are safe enough should the '200 mm break' occur in one cold leg of the primary circuit. Namely, about 150 K safety margin for the peak cladding temperature of the nuclear fuel has been calculated, considering the upper bound of the performed uncertainty analysis.

1 INTRODUCTION

Kozloduy-3 and 4 (Fig. 1) are 6 loop 1375 MWth WWER 440/230 units, designed by Gidropress in Russia in the '60-ies and put into operation respectively in 1980 and 1982. The units are owned and operated by the "NPP Kozloduy plc" in Bulgaria.

The main safety features of these units are:

- Highly reliable SCRAM system (absorber assemblies fall into the core by gravity);
- Low Pressure and High Pressure Safety Injection systems (3 independent trains each);
- Large inventories of primary and secondary coolant in the six loops with horizontal Steam Generators;
- Lower linear thermal load in the core, compared to western PWRs.

The conclusions of the first IAEA OSART mission in 1991 set the basis for an extensive modernisation program [1], initiated by NPP Kozloduy with the purpose to bring these units up to the modern international safety standards. The program is financially supported by the EC, EBRD, DOE of USA, WANO and other international institutions. The scientific and engineering basis of the program is developed mainly by Energoproekt plc and other Bulgarian engineering companies. A significant part of the activities in the frame of the program is the re-evaluation of the plant safety, considering the performed hardware modifications and the evolution of the international safety standards [2]. This paper presents the analyses, performed for definition of the new Design Basis Accident for units 3 and 4.

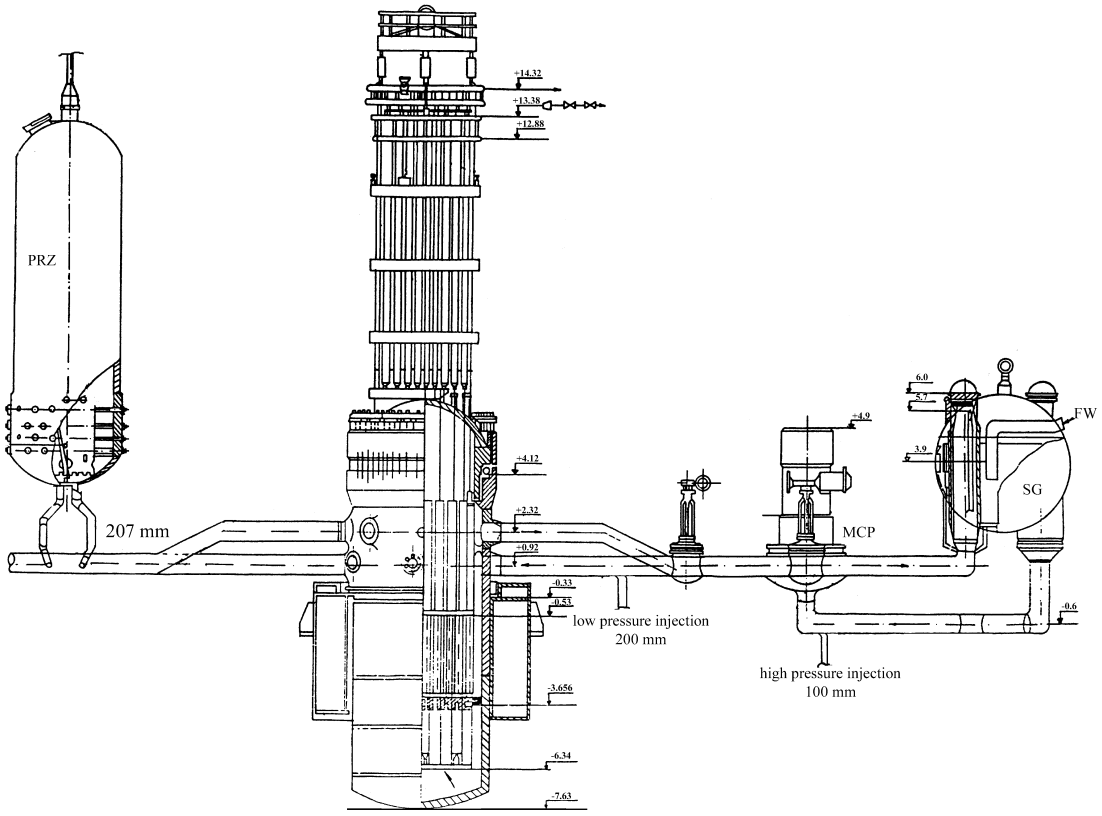


Fig.1. NPP "Kozloduy" units 3 & 4 (WWER-440/V-230) — general layout.

2. INITIAL SET OF ANALYSES

The initial set of analyses is performed by Energoproekt-plc [3].

2.1 Selection of most conservative break location and timing

The possible locations of a break with 200 mm equivalent diameter are, as follows:

a. rupture of a LPI line (**Cold Leg** LOCA)
b. rupture of a Pressurizer surge line, which results in LOCA 2x207 mm on the **Hot Leg.**

Several calculations are performed with different boundary condition for both locations in order to evaluate the most conservative set of plant specific initial and boundary conditions:

⇒ core power distribution in the Beginning and End of the Fuel Cycle (BOC & EOC) **EOC status is finally assumed**

⇒ break location — **rupture of a LPI line (Cold Leg LOCA) is finally assumed**

⇒ break flow discharge coefficients — **maximal values are assumed**

⇒ time of assumed Loss of Off-Site Power (LOOP)

LOOP is assumed at the time of SCRAM actuation signal

All other initial and boundary conditions are postulated following the IAEA guide [2]:

- one of the three ECCS trains is assumed to fail and one of them is supposed to inject into the break in case of LPI line rupture, i.e. **only one train is considered operable.**
- hot rod is modeled in the hot core channel, with power load derived from the maximum acceptable linear heat flux: 325W/cm
- the nominal unit parameters are used as initial conditions with conservative corrections, reflecting the measurement uncertainty
- decay heat is conservatively assumed equal to ANS71 +20%
- maximal peaking factors are used for fuel assembly with maximal rod linear heat flux;
- a conservative ECCS tank water temperature profile is calculated and used
- constant atmospheric pressure is assumed in the confinement.

2.2. Acceptance criteria

The limiting acceptance criterion is selected, considering the IAEA guidelines [2] and the relevant Bulgarian regulations [4]: Peak cladding temperature of the fuel **PCT < 1200 °C**.

2.3. Primary and secondary side modeling

An important feature of WWER-440/V-230 is, that in case of LOOP, two MCP-s run down on their own inertia and stop in about 10 s (mechanical rundown), while the other four are supplied by Turbine inertial rundown (electro-mechanical rundown) and stop in about 100 s.

The six real loops are represented in the model as three lumped loops:

Loop 1 — represents the real damaged loop, on which the break is postulated. Electro-mechanical rundown is conservatively assumed for this MCP in case of LOOP
Loop 2 — represents the two real loops with mechanical rundown of MCPs
Loop 3 — represents three real loops with electro-mechanical rundown of MCPs

The core is modelled as a system of three channels — bypass, hot channel with a hot fuel rod and an average channel, which represents the rest of the core.

The energy-release part of the fuel elements is modeled by five axial sectors. The downcomer of the reactor is divided into three parts according to the loops model. The SG tube bundle is represented by five axial sectors considering its relatively low impact during large LOCA.

The model is revised in detail and approved by experts from INEEL laboratory (USA). The adequacy of the modeling is checked against the requirements for modeling of reactor facilities using this code (RELAP5) as well as the correctness of input data interpretation.

A special engineering analysis of the differences between unit 3 and unit 4 is performed, resulting in the selection of unit 3 as a reference unit for the calculations.

2.4. Results of the calculations

The events sequence is given in Table 1, and significant parameters trends are shown in Figs 1 to 5.

Table 1. EGP analysis: imposed sequence of main events

Event	Time, s
1. LPI line rupture. LOCA 200 mm on the Cold Leg	0.0
2. Signal "Primary side pressure below 11.15 MPa"	2.0
3. Actuation of SCRAM by the signal in p.2; LOOP assumed. Closure of Turbine Stop Valves actuated. MCP-s rundown (2 MCP-s – mechanical and 4 MCP-s – electromechanical). SG FW isolation actuated.	3.5
4. One HPIP starts to inject into the primary circuit	58.0
5. Signal "Primary side pressure below 0.792 MPa". One LPI Pump starts to inject into the primary side	320.0
6. Maximal temperature of the fuel cladding PCT ≈ 810 °C	574.0
7. Stabilized core cooling	670.0

As a result of the break flow, the primary pressure drops down to the set point of SCRAM actuation. Loss of off-site power (LOOP) is assumed at SCRAM, causing TSV closure, termination of the SG feed water supply and the MCP rundown.

In spite of the injection with 1 HPIP, which starts 56 s after the LOOP, the loss of primary coolant through the break causes further decrease of the core level.

At 280 s, the level becomes critically low and the flow rate of the generated steam is not sufficient to cool the core effectively. As a result, the fuel rod cladding temperature starts to increase, achieving a maximal value of $T_{cl} \approx 810°C$ at 574 s.

The fluid level in the core reaches its minimum value at 420 s. Afterwards it starts to rise as a result of the LPIP actuation. The water delivered by the ECCS changes the heat transfer mode in the core. At time equal 574 s, the quench front reaches the fuel rods area, causing a sharp decrease of the cladding temperature.

The acceptance criteria of PCT < 1200^{o}C is satisfied by a large margin (≈ 400^{o}C).

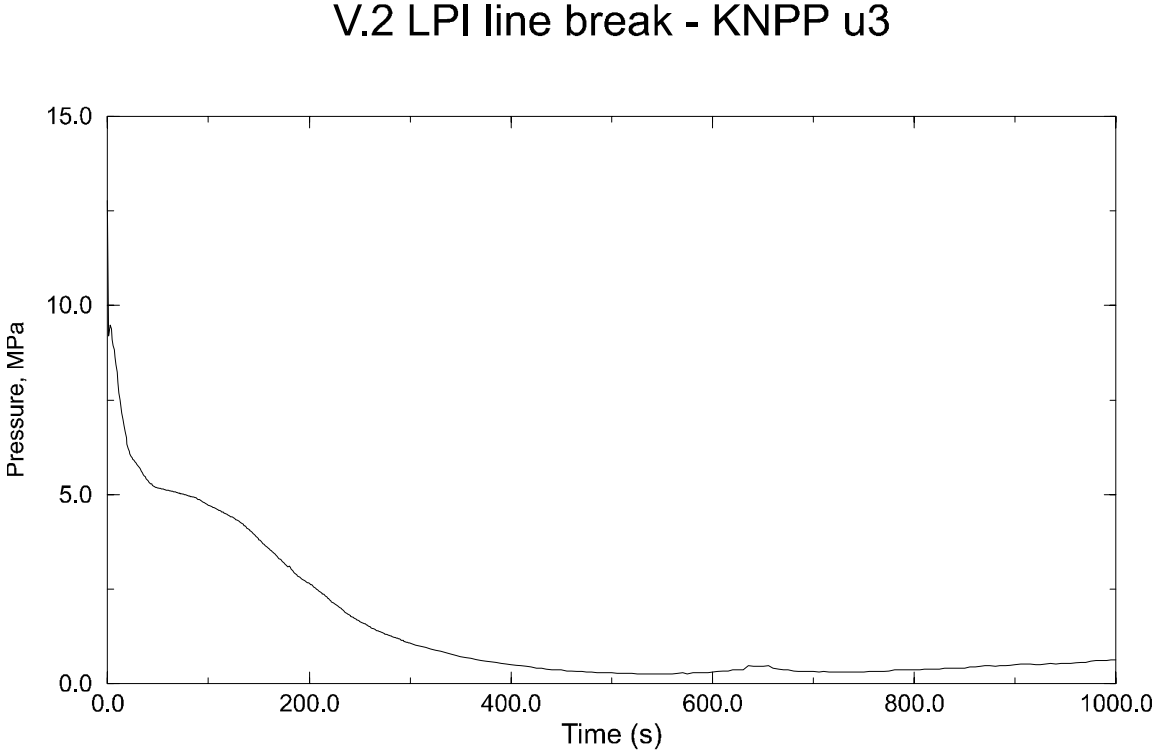


Fig. 1. EGP analysis: PS pressure.

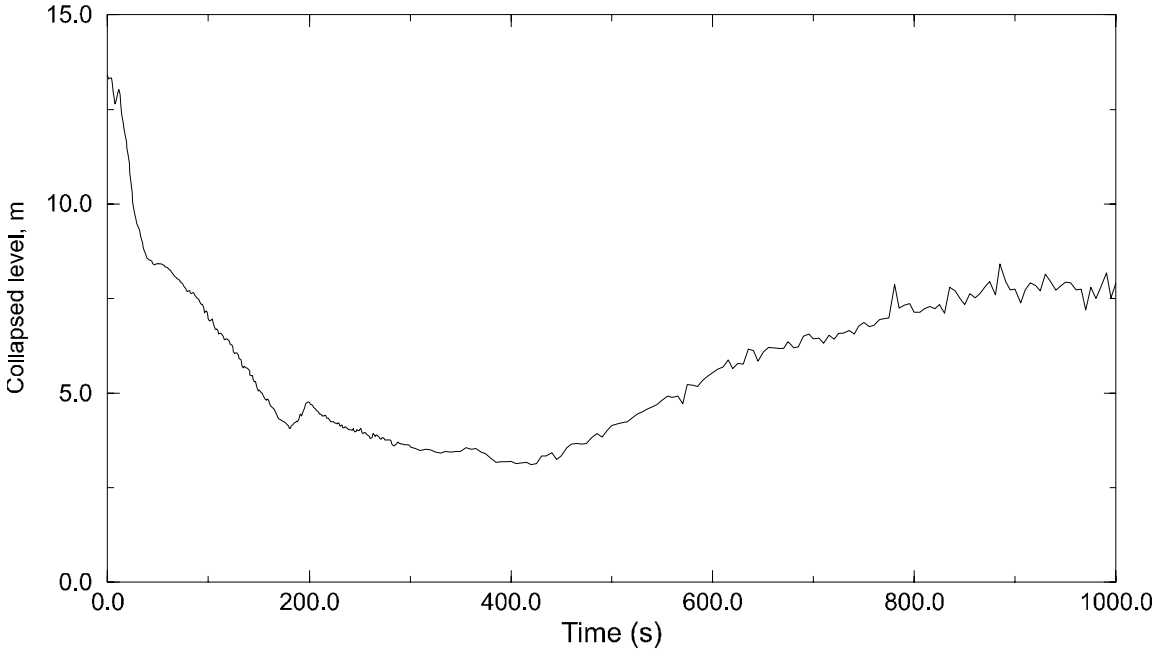


Fig. 2. EGP analysis: RPV collapsed level.

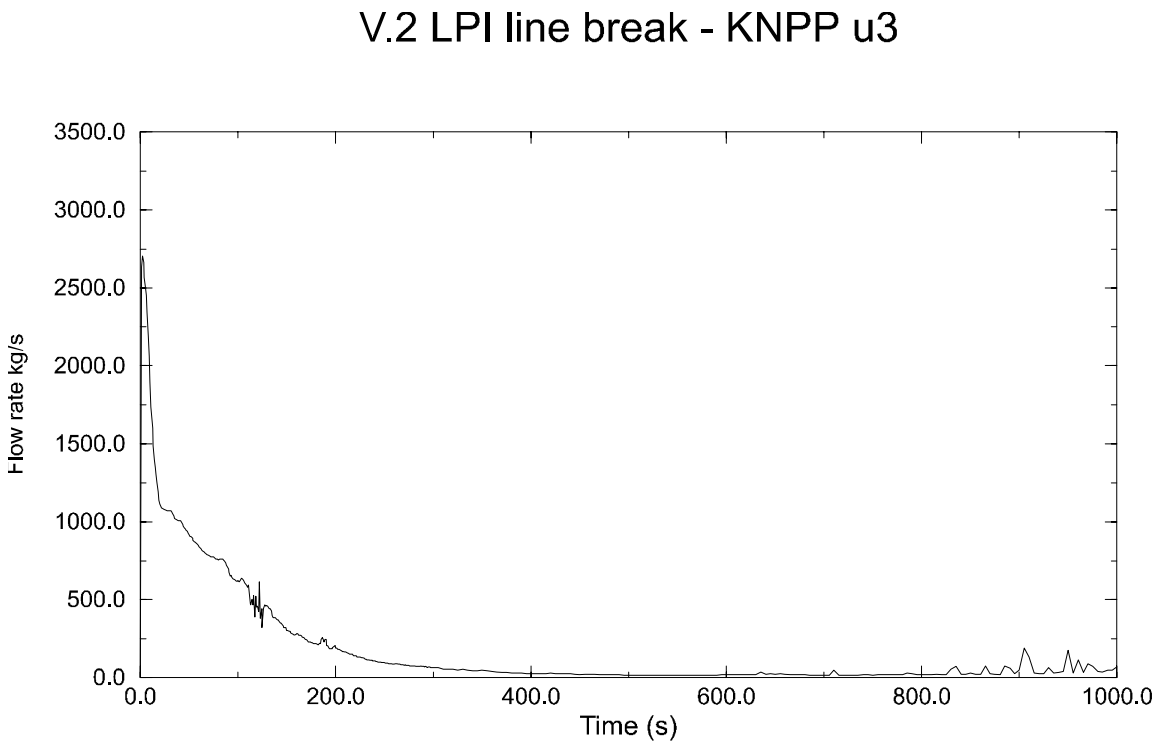


Fig. 3. EGP analysis: Break flowrate.

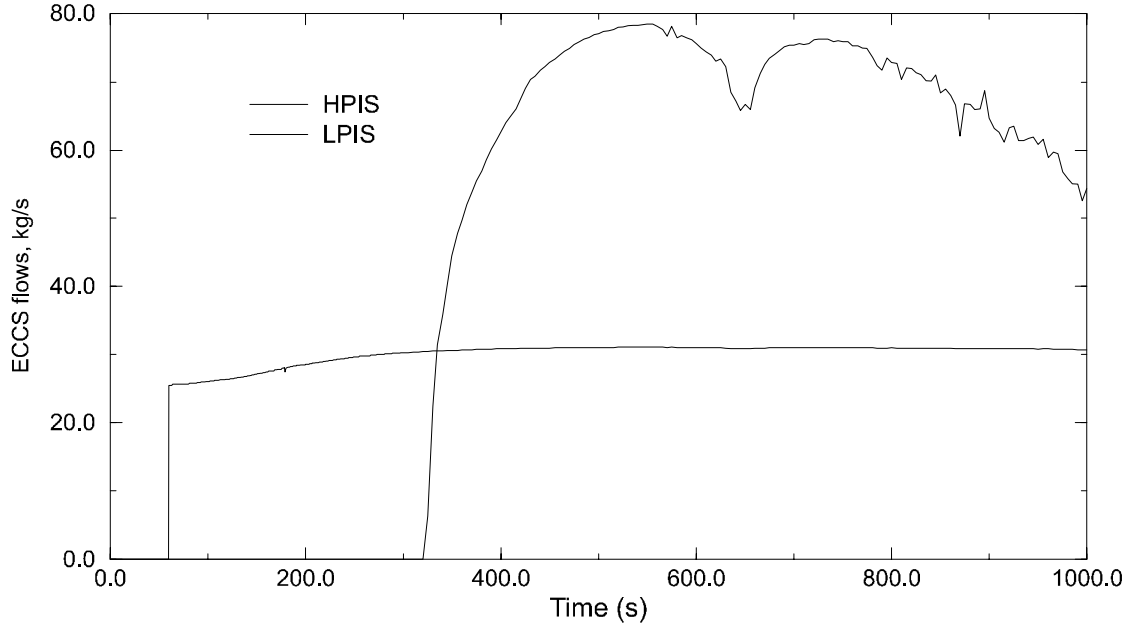


Fig. 4. EGP analysis: ECCS flowrate.

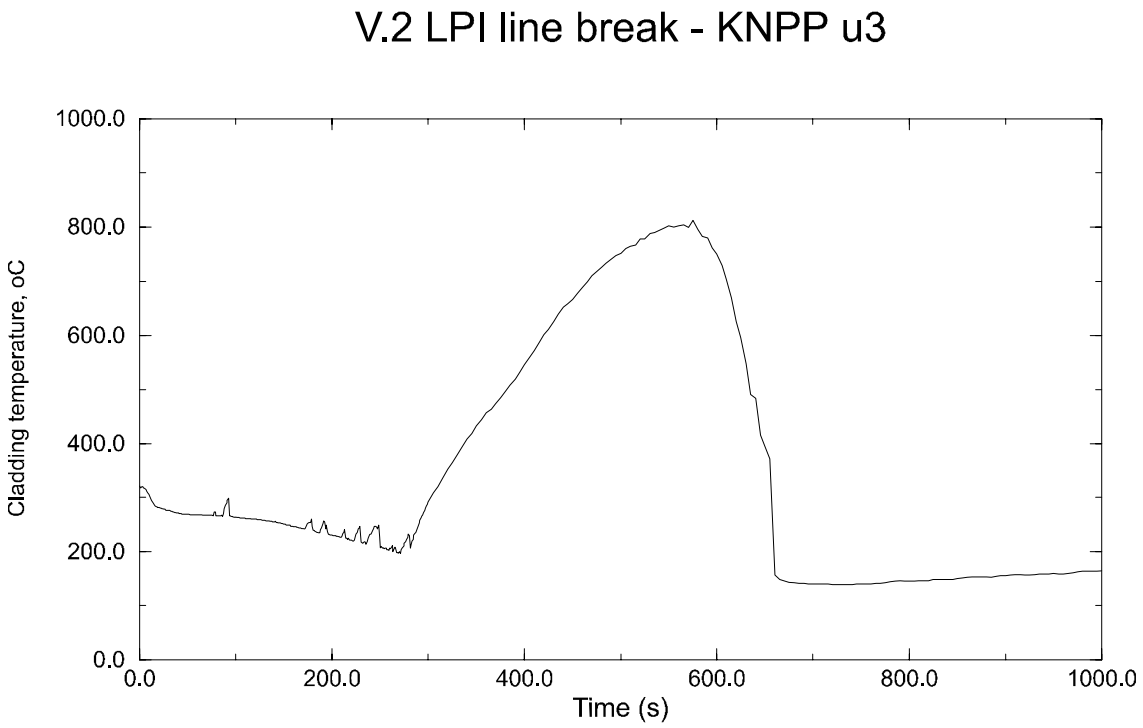


Fig. 5. EGP analysis: maximum clad temperature. hot rod.

3. INDEPENDENT BEST ESTIMATE ANALYSIS WITH RELAP5/Mod3.2 [5]

Considering the great importance of the analyses and the necessity for a sound justification of the results before presentation to the regulatory body, NPP Kozloduy-plc initiated a special project in cooperation with the Department of Mechanical, Nuclear and Production Engineering of the University of Pisa (DIMNP) for an independent review and evaluation of the results.

3.1. Nodalisation development

The nodalisation for the calculations with RELAP5/Mod3.2 is independently developed by DIMNP, on the basis of documented plant data. Considering the specific task of LOCA analysis, the deck includes some LOCA-specific features:

a. 3-D approach to the reactor vessel modeling
b. Relatively coarse noding of the SG.

The main characteristics of the nodalisation are presented below:

- Each of the six loops is modeled separately
- The core region is subdivided into six parallel hydraulic regions (including bypass). Seven parallel stacks are modeled to calculate heat transfer inside the active fuel rods
- The downcomer region is separated into six regions, each region attached to one cold leg. Cross flow junctions allow azimuthal flow among the regions
- The break is modeled on loop No 1. The pressurizer is connected to loop No 6

- The full ECC system is modeled including three HPIP and three LPIP injecting separately into all loops and in loops 1, 3 and 5, respectively. Injection locations and flow-rates are modeled according to the documented plant data
- A relatively simplified noding for the secondary side of the steam generator is considered. This includes three layers of horizontal tubes and is assumed to be sufficient for the simulation of large break LOCA
- The behavior of the steam lines and of the feed-water lines is simulated by proper boundary conditions.

In the frame of the Kozloduy assistance project, the nodalisation is used for Best Estimate (BE) analyses under realistic or conservative Boundary and Initial Conditions (BIC) for analysis of DBA and BDBA LOCA accidents. Conservative BIC are applied to the case of **LOCA 200mm on the Cold leg**, which is analyzed as a DBA for the concerned units.

3.2. Qualification of the nodalisation

In order to qualify the nodalisation at the "steady-state" level, a transient calculation is performed without imposing any variation to the input parameters (a null-transient). The suitable duration for the null-transient is fixed as 100 s. The results achieved at the end of the 100 s calculations are used to evaluate the nodalisation quality. The steadiness of the solution is checked and demonstrated to be consistent with the acceptability threshold. An abstract of the results from the qualification process are presented in Table 2.

Qualification at "on-transient" level should be performed next, in order to show the correct modeling of BIC, which could not be checked at the 'steady-state' level. In this project this goal is achieved by comparison to results of Energoproekt-plc RELAP and DIMNP CATHARE calculations. Besides, this nodalisation is successfully applied for simulation of a small LOCA experiment in the frame of another DIMNP project for WWER [6].

3.3. Calculation and results

The independent calculation with RELAP5/Mod3.2 is performed with the following conservative values of the main input parameters:

Table 2 Abstract from the DIMNP, Steady State Nodalisation Qualification results [5]

No.	QUANTITY	ACCEPTABLE ERROR (°)	REFERENCE VALUE	RELAP5	ERROR
1	Primary circuit power balance	2%	1430 Mw	1430 Mw	0%
2	Primary system max pressure	0.1%	126 bar	125.6 bar	0.3%
3	Steam Generator exit pressure	0.1%	47.6 bar	45.2 bar	5%
4	Steam Generator feedwater temperature	0.5%	493 K	496 K	0.6%
5	Pump velocity	1%	153.94 rad/s	152.9 rad/s	0.6%
6	Primary system total loop coolant mass flow rate	2%	12.11 m^3/s	11.31 m^3/s	6%
7	Steam Generator total mass flow rate (6 loops)	2%	750 kg/s	781 kg/s	4%
8	Core coolant mass flow rate (active region)	2%	10.89 m^3/s	10.33 m^3/s	5%
9	Core bypass mass flow rate (LP-UP)	10%	1.21 m^3/s	0.98 m^3/s	19%
10	Pressurizer level	0.05 m	5.6 m	5.59 m	0.01 m
11	Secondary side or downcomer level	0.1 m	1.919 m	1.647 m	0.272 m

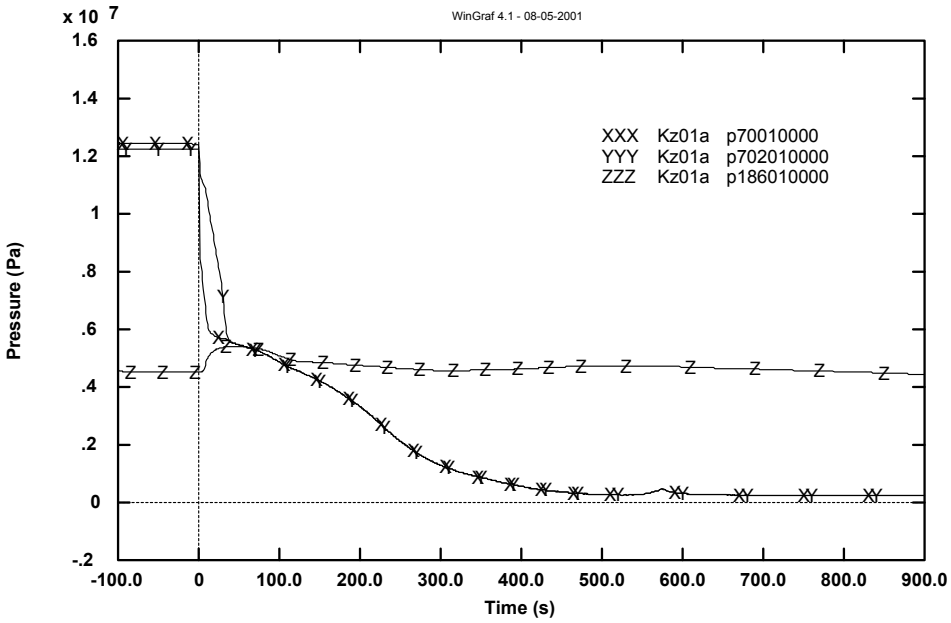


Fig. 6. DIMNP analysis: Pressure in UP (XXX), PRZ (YYY) and SG1 (ZZZ).

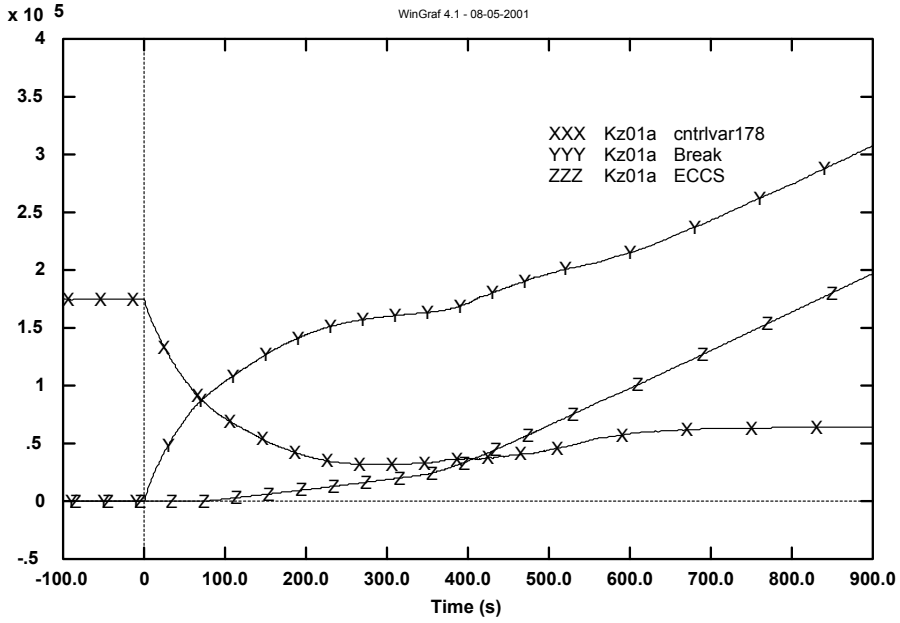


Fig. 7. DIMNP analysis: Mass inventory in PS (XXX) and flowrate integrals of the break and of ECCS injection.

Core power is assigned to be 1430 instead of 1375 MWth

1) The Peak linear power for the 'realistic hot rod' (HRR) is assigned 34.2 KW/m, while ref. [7] suggests 29.5 KW/m as 'realistic' and 32.5 KW/m as 'permissible'

2) The core power decay is assigned equal to 1.20 times the 'ANS 79' values

3) Conservative (about 5% lower than realistic) values have been assigned to the flow-rates delivered by the High Pressure and Low Pressure safety injection pumps.

The calculation results are presented in Figs. 6 to 8. The PRZ pressure remains above the UP pressure up to about 30 s transient time due to two-phase critical flow occurrence in the surge line. The primary mass inventory achieves a minimum of about 20% of the nominal value at 280 s, causing degraded core cooling conditions. Afterwards, the ECCS actuation recovers the primary coolant inventory to about 60% of the nominal value at about five minutes transient time. This establishes suitable core level (and then core cooling), which remains stable till the end of the calculated time period.

As expected, the SGs play a minor role for the transient evolution: exchanged thermal power across SG becomes smaller than core power early into the transient and much lower than the thermal power exiting with the break flow.

The calculated transient progression **is significantly different** from a typical LB-LOCA in Western PWRs. This is explained by the following **specific features of WWER-440/V230:**

a) The **AR/V (break area over primary system volume) ratio** equals 1.30e-4 m^{-1}**.** This is almost **ten times smaller** than the value typical for LB-LOCA in PWRs

b) The '**electro-mechanical MCP rundown**' causes flow reversal in the two loops with '**mechanical run-down**' during the first minute of the transient. MCPs have minor effect during LBLOCA in PWR

c) The maximum allowed **linear power** for the nominal operation that ranges up to about 50 kW/m in Western PWR and remains below 33 kW/m in WWER 440/V230

d) The presence of **accumulators** in Western PWR, which mitigate the transient evolution during the first tens of seconds. The Kozloduy WWER 440/V230 do not have such devices

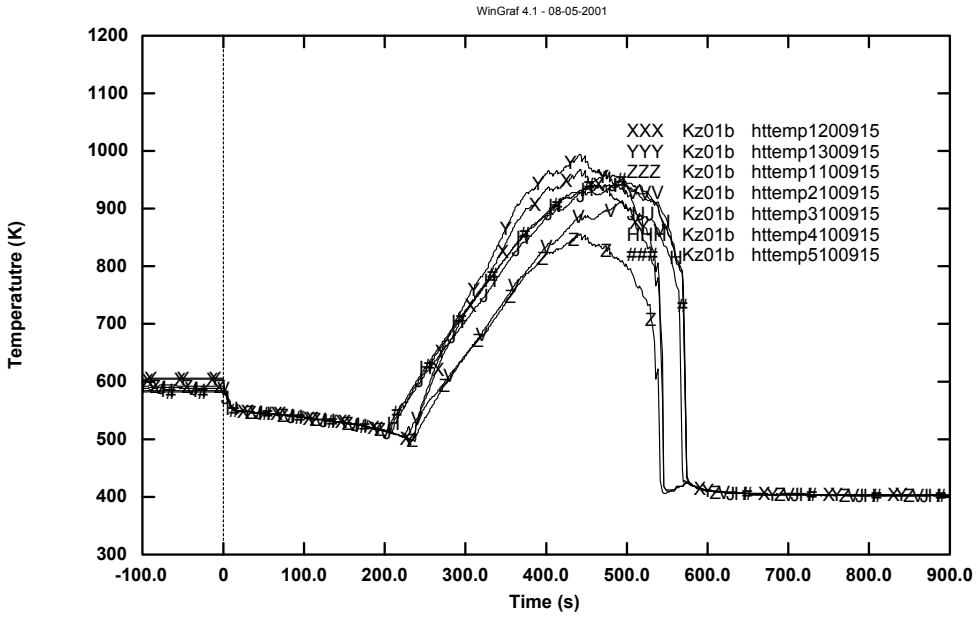


Fig. 8. DIMNP analysis: PCT for different fuel rods included in the nodalisation.

4. COMPARATIVE CALCULATION WITH CATHARE [5]

The purpose of the comparative calculation is to demonstrate the independence of the main result (PCT<1200 °C) from the code-specific characteristics of RELAP5/Mod3.2. Such a demonstration could prove the units capability to withstand LOCA 200 mm as DBA.

4.1. Nodalisation development

The same considerations for the development of nodalisation are adopted for the independent calculation with RELAP5/Mod3.2, apply here. The same activities are performed in the construction of a reference nodalisation for LBLOCA for CATHARE. The same database related to the Kozloduy unit 3 NPP is used. The main features of the nodalisation are presented below:

Two loops (A and B) are modeled separately, each loop including HL, SG, MCP and CL.
The loop A represents the loops 2 & 4 of the Kozloduy unit 3 NPP and the loop B represents the loops 1 & 3 & 5 & 6. The rationale at the basis of the subdivision derives from the MCP performance following LOOP. MCP of loops 2 & 4 are characterized by the mechanical run-down (or coast-down) that causes MCP rotational speed to reach the 'zero' value in about 10 s. MCP of loops 1 & 3 & 5 & 6 are characterized by the electro-mechanical run-down that causes MCP rotational speed to reach 'zero' value in about two minutes (100 s). Differences in run-down speed affect flowrates in hot and cold legs and in core region and determine the cooling of the core during the blowdown period of LBLOCA.

The pressurizer is installed in loop A and the break in the case of LBLOCA analyses is assumed to occur in the CL of the loop B.

The general features of the CATHARE nodalisation, apart from the loop subdivision, resemble the general features of the RELAP5 nodalisation with the two following exceptions:

a. The core region is modeled by a lower number of parallel channels in compliance to the CATHARE 2 manual that requires the execution of subsequent calculations to calculate rod surface temperatures in selected fuel elements or fuel rods
b. The secondary side of the steam generators is modeled by a single, upward oriented volume and not by two stacks of nodes. This derives from the 'confirmatory nature' of the present CATHARE analysis

The standard CATHARE procedure is adopted to achieve the steady state and the stabilization of the relevant thermalhydraulic parameters.

The CATHARE nodalisation is used only under conservative Boundary and Initial Conditions (BIC) for the analysis of LOCA 200mm on the Cold leg, — as a DBA for the concerned units.

4.2. Qualification of the nodalisation

In order to qualify at the "steady-state" level, the CATHARE nodalisation is subjected to the same procedure as the RELAP5 nodalisation. The results achieved at the end of the 100 s calculations are used to evaluate the nodalisation quality. The steadiness of the solution is checked and demonstrated to be consistent with the acceptability threshold.

4.3. Calculation and comparison with RELAP5 (initial and independent calculations)

The CATHARE calculation is performed with the same conservative values of the main input parameters, as for the independent RELAP5/Mod3.2 calculation, performed by DIMNP [5]. If one takes the DIMNP calculation performed by RELAP5 (Independent Analysis) as reference scenario for the 'LBLOCA 200 mm' in the Kozloduy unit 3 (this is justified by the consideration that uncertainty analysis has been carried out), the only possible conclusion is that the overall transient scenarios predicted by EGP (Initial Licensing Analyses), DIMNP-RELAP5 and DIMNP-CATHARE are qualitatively and quantitatively similar. This is substantiated by the results in Figs. 9 and 10 and Table 3. This conclusion shows that the differences in input conditions adopted by the three calculations, which are emphasized in the previous sections, give a negligible contribution to the predicted time trends and constitute an evidence of the capabilities of the code users in performing the considered studies.

Additional specific remarks related to the comparison among the three calculations are summarized hereafter:

- An 'unknown' part of the discrepancies between the three predictions must be attributed to the lumping or separating the loops of the primary system. Mainly occurrence of liquid flow at the break is largely affected by this user choice
- The adopted linear power and the connected peak factors constitute the other major source of discrepancy between the three predictions. In the case of CATHARE only two parallel stacks of nodes have been adopted and the HRR is not modeled
- An early dryout occurrence can be noted in the CATHARE calculation compared with the two RELAP5 calculations (items 19 to 25 in Tab. 3 and Fig. 10). This may be related partly to the different hydraulic behavior of the system originated by the 'lumping' of the loops (discussed above) and partly by the different criteria (possibly more conservative) adopted by the CATHARE model to characterize the CHF event.

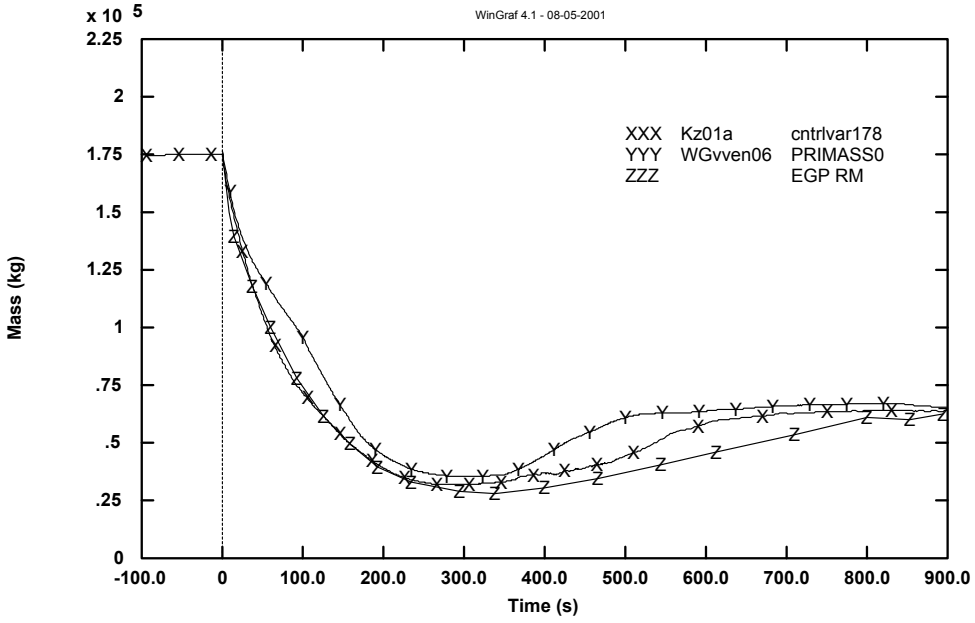


Fig. 9. Comparison of DIMNP CATHARE results with EGP RELAP5 and DIMNP RELAP5: coolant mass inventory in primary system.

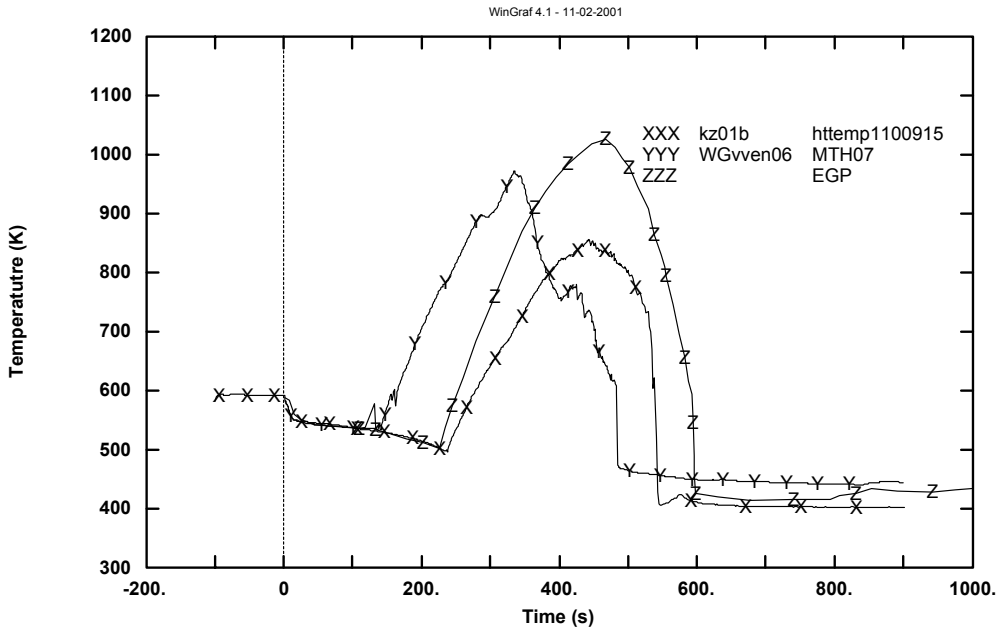


Fig. 10. Comparison of DIMNP CATHARE results with EGP RELAP5 and DIMNP RELAP5: Fuel rod surface temperature in hot channel.

Table 3. Comparison between the resulting sequences of main events

No	EVENT	UNIT	RELAP5 EGP	RELAP5 DIMNP	CATHARE2 DIMNP
1	Break opening	s	0	0	0
2	Scram (CR start to move/CR fully inserted)	s		1.7/14.7	1/-
3	MCP trip (start/end of coast-down), mechanical	s		3.2/13.2	3.2/13.2
4	MCP trip (start/end of coast-down)	s	3.6/-	5.7/196	5.7/196
5	FW isolation (start/end)	s	3.6/-	2.7/33	2.7/33
6	Steam Line isolation (start/end)	s		3.2/8.2	3.2/8.2
7	PRZ emptying (level below 0.15 m)	s		29	14
8	Actuation of HPIP	s	60	74	74
9	Actuation of LPIP	s	311	351	351
10	Minimum mass in primary loop (tons and% of initial value)	tons/%	29/-	32/18	35/20
11	Occurrence of minimum mass in primary loop	s	310	282	300
12	PCT in Central Fuel Assemblies	K	1073	914	991(*)
13	PCT in Average Core Region, part 1	K		953	
14	PCT in Average Core Region, part 2	K		945	
15	PCT in Peripheral Fuel Assemblies	K		958	
16	PCT in hot fuel bundle of Hot Hydraulic Assembly (HHA)	K		856	1074 (°)
17	PCT in ‘hot rod realistic’ (HRR) in HHA	K		968	
18	PCT in ‘hot rod conservative’(HRC) in HHA	K		995	
19	PCT occurrence in Central Fuel Assemblies	s	442-470	495	372 (*)
20	PCT occurrence in Average Core Region, part 1	s		495	
21	PCT occurrence in Average Core Region, part 2	s		495	
22	PCT occurrence in Peripheral Fuel Assemblies	s		474	
23	PCT occurrence in hot fuel bundle of HHA	s		443	340 (°)
24	PCT occurrence in ‘hot rod realistic’ in HHA	s		443	
25	PCT occurrence in ‘hot rod conservative’ in HHA	s		443	
26	Calculation end	s	1000	900	900

(*) Medium channel in CATHARE2 nodalization (°) Hot channel in CATHARE 2 nodalization

5. UNCERTAINTY ANALYSIS AND SENSITIVITY STUDY [5]

The code limitations and the approximations, introduced within the process to produce the transient prediction, make the uncertainty evaluation a necessary element of a BE study. Within the present context, the uncertainty evaluation of the independent RELAP5 analysis allows the quantitative evaluation of the initial analysis results.

5.1. Overview of the CIAU procedure

The methodology based upon CIAU (Code with capability of Internal Assessment of Uncertainty), has been adopted in the present framework for uncertainty evaluation. The number of experiments that are used to derive code uncertainty is still limited. Therefore, a sensitivity study has been executed to confirm the results obtained from this methodology.

CIAU is described with suitable level of detail in ref. [7]. A summary description of the methodology is reported hereafter.

Uncertainty is the measure of the precision, or of the error, that characterizes a generic calculation or a measurement. Referring to the calculations, uncertainty affects the results of the prediction obtained by any numerical tool. Uncertainties may have different origins ranging from the approximation of the models, to the approximation of the numerical solution, to the lack of precision of the values adopted for boundary and initial conditions. Different uncertainty methodologies have been developed recently, e.g. the CSAU (Code Scaling, Applicability and Uncertainty) methodology, proposed by the US NRC. All of the uncertainty methodologies suffer of two main limitations:

The resources needed for their application may be prohibitive — up to several man-years;

The achieved results may be strongly methodology/user dependent.

The last item, together with the code-user effect, may threaten the practical applicability of the uncertainty evaluation results. Therefore, the Internal Assessment of Uncertainty (IAU) ‘capability’ has been proposed in order to remove the above limitations.

The idea at the basis of the CIAU can be summarized in two parts:

1. each plant status is characterized by the value of six relevant quantities (i.e. a hypercube) and by the value of the time since the transient start
2. association of uncertainty values to each predicted plant status

In the case of a PWR the six quantities that identify a hypercube are: a) the upper plenum pressure, b) the primary loop mass inventory, c) the steam generator pressure, d) the cladding surface temperature at 2/3 of core active height, e) the core power, f) the steam generator downcomer collapsed liquid level.

Let us define Y as the generic calculation output reported as a function of time. Each point value in the curve is affected by a quantity error (Uq) and by a time error (Ut). Owing to the uncertainty, each point value may take any value within the rectangle identified by the quantity and the time errors. The amount of error can be defined in probabilistic terms. This is consistent with the NRC licensing approach (the 95% probability level is considered acceptable for comparison of best estimate predictions to the licensing limits).

The *idea* at the basis of CIAU can be made more specific by the following statement: *the uncertainty in code prediction is constant within each plant status.*

Additional considerations are:

- Uncertainty data are continuously gathered and combined, in the same way as the CHF look-up tables proposed by Groeneveld, are set up and qualified
- Each transient evolves throughout a series of subsequent status. Every time the event touches a hypercube and a time interval (i.e. a plant status), it takes proper uncertainty values. In this way, the entire event can be associated with uncertainty bands.

The development of Internal Assessment of Uncertainty requires a qualified system code and a suitable uncertainty methodology. The following items are necessary:

- qualified experimental data
- qualified system codes calculation results
- postulated transients including the definition of plant status
- selection of variables in relation to which the uncertainty must be calculated.

CIAU Application:

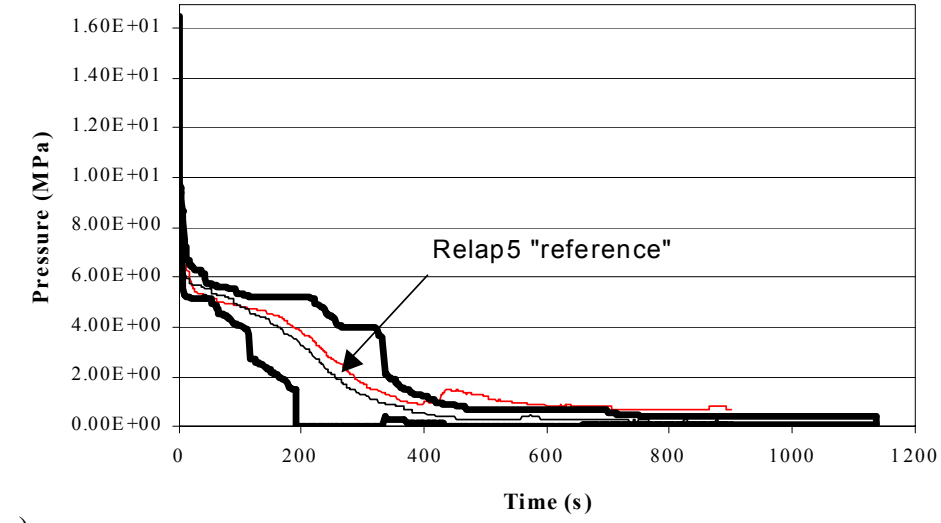
The ASM (Analytical Simulation Model), i.e. a qualified NPP nodalisation, is used to produce the transient prediction. Once a generic event is predicted, the six driving quantities are used to identify the succession of hypercubes. The time intervals are identified by the predicted events timing. This leads to the quantity uncertainty and the time uncertainty values. A special computer tool is used to combine time and quantity uncertainty at each time of the predicted event. Continuous uncertainty bands are generated to envelope the ASM calculation results.

5.2. Results from the CIAU application

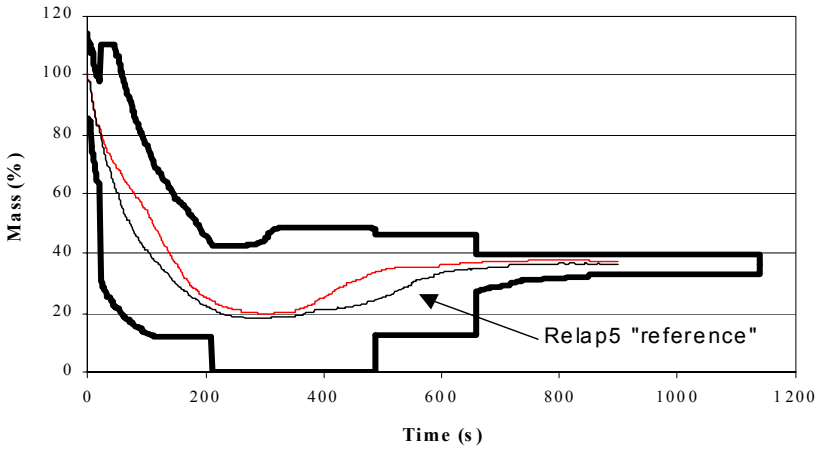
In the case of the Kozloduy NPP unit 3 LBLOCA, the input deck ‘kz01’ used in the independent RELAP5 analysis, is assumed as the actual ASM and related results are adopted in the CIAU application.

Automatic uncertainty bands for the three parameters of interest, i.e. I-ry pressure, I-ry mass inventory and rod surface temperature at 2/3 of the core active height, are generated by the CIAU and constitute the results of the application. These are given in Figs 11 a), b) and c) where, for comparison purposes, CATHARE results are also reported.

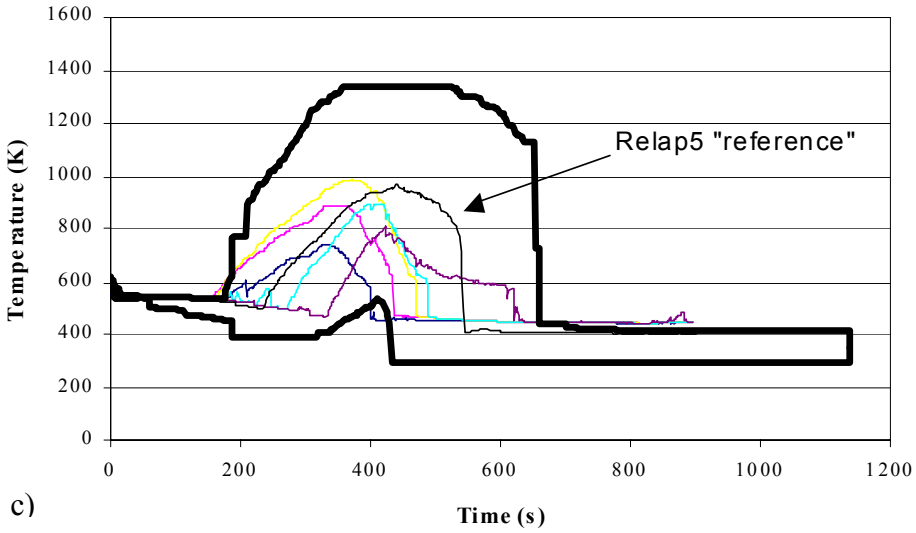
Uncertainty bands indicated in the above figures may assume different meanings or implications. One of these is that the actual system behavior, should the ‘LBLOCA 200 mm’ occur, is bounded by the upper and lower curves characterizing the uncertainty evaluation with 95% probability (with 95% confidence limit). Another implication is that any different BE code prediction (still same input assumptions as the reference calculation) should be bounded by those limits. This last implication is considered related to the CATHARE calculation. Figures 11 a), b) and c) show that CATHARE prediction is actually bounded by the uncertainty limits derived for the RELAP5 prediction. This can be considered a necessary condition (actually the only one) to demonstrate the similarity between transient scenarios predicted by two different calculations.



a)



b)



c)

Fig. 11. CIAU results related to the DIMNP RELAP5 calculation and demonstration that CATHARE results 'are bounded' by the uncertainty bands related to the RELAP5 calculation.

5.3. Sensitivity study

The objective of the sensitivity studies is to support the uncertainty evaluation of CIAU.

Starting from the 'reference' nodalisation, single parameters are varied in each code run. Six groups of input parameters are distinguished including 'FUEL', 'NODALISATION', 'LOOP HYDRAULICS', 'PSA AND ECCS', 'NEUTRONICS', 'OTHER'. Nineteen variations of input parameters are considered within the present framework. Detailed information about the results can be found in refs. [5] and [6].

Several safety relevant parameters can be considered to evaluate the results of the sensitivity studies. The attention is focused in ref. [5] to □PCT and □t_{CHF}, making reference to the behavior of the 'hot rod realistic' (HRR) at the axial level 9. The (□) parameter is defined as the difference between the reference calculation (run 'kz01') value and the one obtained from the sensitivity run. Exemplificative results, related to rod surface temperature are shown in Fig. 12.

The following results from the sensitivity study can be emphasized:

- The influence of material and geometric properties of the fuel upon safety relevant parameters is limited because the dry out occurrence is affected to a limited extent by the thermal energy release from the fuel
- Worst conditions for core cooling are predicted when the break is located in loop No 3
- Break flow area has a strong influence on the results
- PSA studies should be performed for the ECCS reliability, which is of a vital importance for the safety of the Kozloduy WWER-440/230 NPP

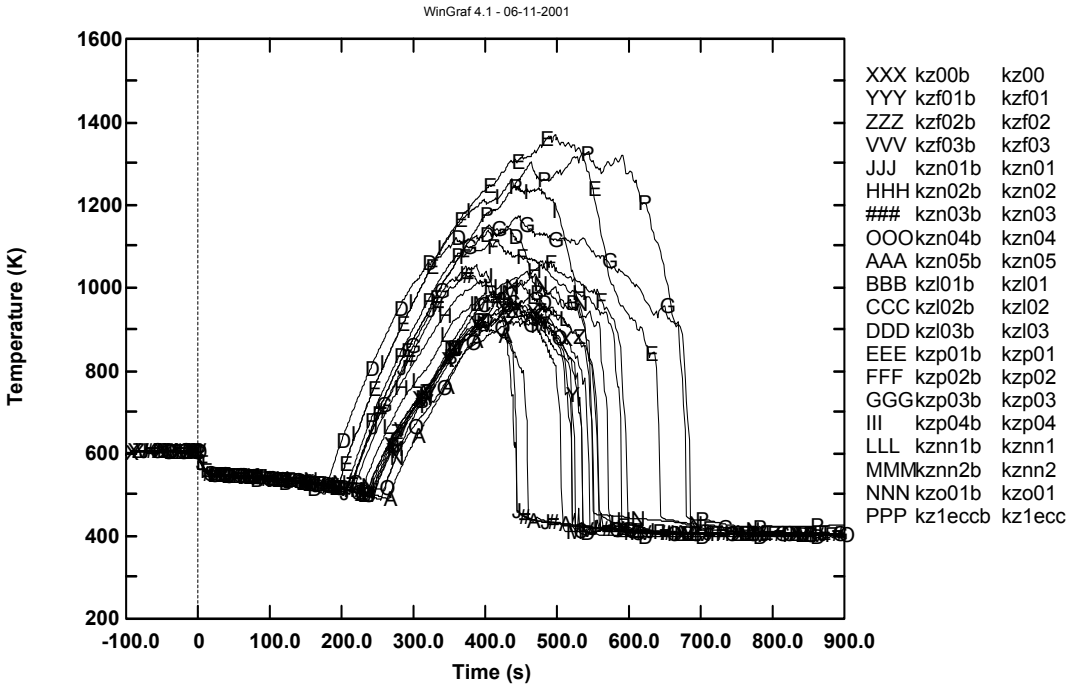


Fig. 12. Results from RELAP5 sensitivity studies related to the Kozloduy unit 3 'LBLOCA 200 mm': envelope of rod surface temperature trends for 'hot rod realistic' from 19 code runs.

6 CONCLUSIONS

The conservatism embedded in the reference calculation, the performed CIAU uncertainty study and sensitivity study, support the conclusion of the initial licensing analyses:
Kozloduy unit 3 is safe in case of LB-LOCA originated by a 200 mm break, provided a minimum number of ECCS come into operation. (Fig.13). This conclusion is deterministic and does not involve any evaluation of the ECCS reliability.

The versatility of the developed DIMNP-Relap5 six-loop nodalisation has been exploited. It has been found that the worst position for the break, as far as core uncovery is concerned, occurs when the break is located in loop No 2 and No 3.

The 'PCT licensing' obtained by the use of a BE code including uncertainty evaluation equals 1062 °C and is below the licensing limit of 1200 °C. The removal of the conservatism considered in the process, is expected to bring the predicted 'PCT licensing' below 1000 °C.

The performed sensitivity study also showed that parameters that are influential in LB-LOCA analyses of Western PWR do not affect the Kozloduy unit 3 predicted scenario. Namely, parameters affecting the heat stored into the fuel (e.g. gap conductivity or gap thickness) are not influential because of adequate core cooling in the initial two minutes of the transient. This derives from the (relatively) small break dimension, the low average linear power and the availability of MCP with 'electro-mechanical' run-down.

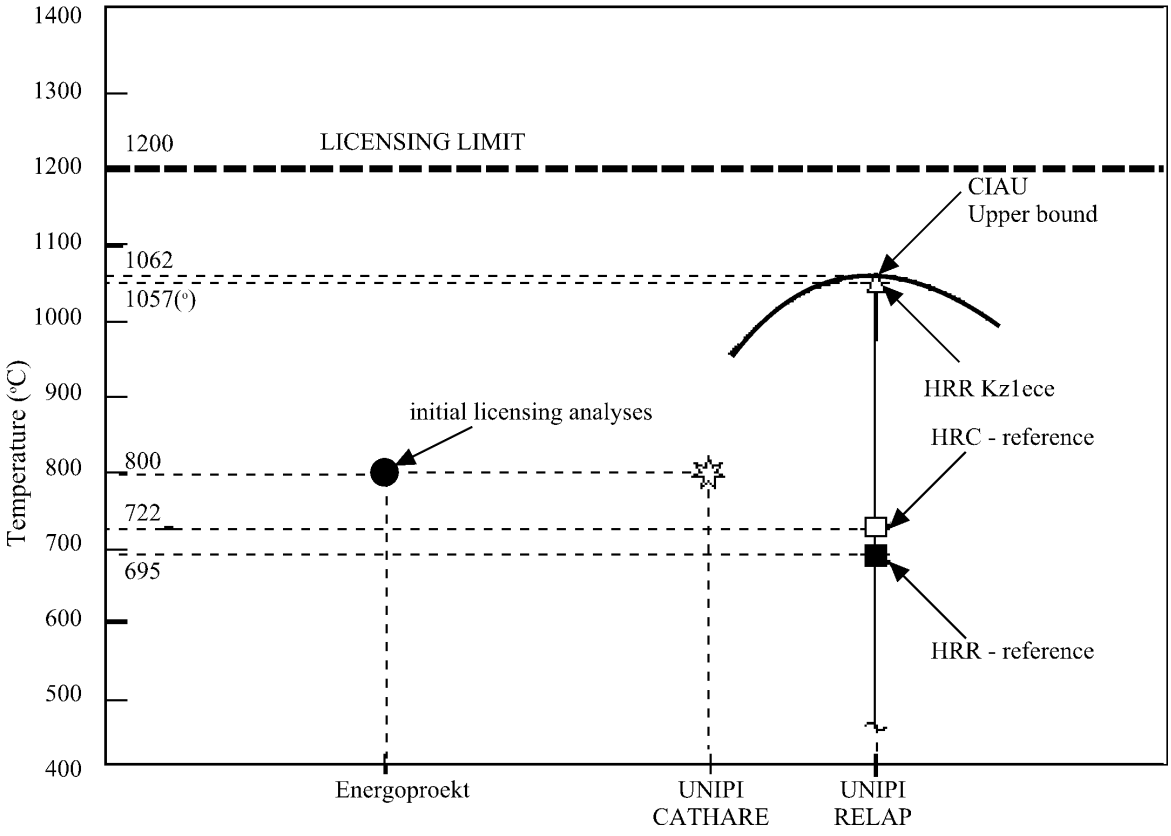


Fig. 13. Comparison between the main results of the study and the licensing limit.

REFERENCES

[1] National Electric Company, NPP"Kozloduy" — units I-IV. Programme'93 for upgrading the operational reliability and safety of units I-IV VVER440 (V230) reactors. May, 1993

[2] IAEA-EBP-WWER-01. Guidelines for accident analysis of WWER Nuclear Power Plants, IAEA, December 1995

[3] Energoproekt plc. A complex set of analyses of accident s with rupture of 200 mm diameter primary sidelines on units I — IV of NPP "Kozloduy". Revision 1, July 2000

[4] Committee for the Use of Atomic Energy for Peaceful Purposes. Order No.3 for provision of the safety of Nuclear Power Plants in their design, building and operation. Bulgaria, Sofia, 1988

[5] D'Auria F., Galassi G.M., Giannotti W. "Confirmatory safety analyses carried out by RELAP5 and CATHARE codes, related to the Kozloduy VVER440/230 unit No.3" University of Pisa Report DIMNP NT 443(01)-rev. 0, Pisa (I) August 2001

[6] D'Auria F., Galassi G.M., Giannotti W. "On-Transient' qualification of Metsamor VVER 440/270 NPP nodalisation" University of Pisa Report DIMNP NT 440(01)-rev. 1, Pisa (I) November 2001

[7] D'Auria F., Giannotti W. "Development of Code with capability of Internal Assessment of Uncertainty" Nuclear Technology, Vol 131, No. 1, pages 159-196–Aug. 2000

DEVELOPMENT OF BEST ESTIMATE ANALYSIS METHODS IN CANADA TO ALLOW QUANTIFICATION OF SAFETY MARGINS

A.N. VIKTOROV
Canadian Nuclear Safety Commission,
Canada

Abstract. The paper presents an outline, from the regulator□s perspective, of the current situation in Canada with development of best estimate and uncertainty assessment (BE+UA) methods intended for application in the licensing safety analysis. Reasons, incentives and expectations related to development and application of the best estimate safety analysis methodology are being explored in some detail. Difficulties in attaining acceptance of this methodology for licensing applications are also discussed. Maintenance of adequate safety margins is a firmly established principle in the Canadian regulatory practice. Safety analysis is performed to demonstrate that margins are present and sufficient. Due to a variety of reasons, some of the operating CANDU□ reactors have been recently experiencing difficulties in compelling demonstration of adequate margins. The industry sees application of the BE+UA safety analysis as a potential way of recovering or improving safety margins and removing operational constraints. The operating power reactors in Canada have been licensed, as anywhere in the world, with the use of deterministic, conservative safety analysis methods. Until now, the conservative approach continues to be the cornerstone of safety analyses. It has been recognized, however, by both the industry and the regulator, that BE+UA methods have reached sufficient maturity to allow more accurate and realistic modelling of accident transients, thus presenting an opportunity to better quantify safety margins. It is expected that in many cases a BE+UA analysis will be able to show larger margins than it was possible to demonstrate using the conservative approach. If the BE+UA analyses predict more benign consequences of analysed events, this would facilitate resolving some of the currently outstanding safety issues and lessen economic penalties on utilities. As a consequence, the industry has started several projects aimed at the development and application of BE+UA methods and has requested the CNSC to evaluate the admissibility of such methods for licensing purposes. In turn, the CNSC has formulated certain expectations, meeting, which would facilitate acceptance of the BE+UA safety analysis. It is believed that following a substantial, initial up-front investment in the development of the methodology and establishing processes for collection and qualification of data, the subsequent effort for performing BE+UA analyses will not be significantly larger than for the traditional conservative analysis. Results of the BE+UA analysis are expected to play an important role in decisions related to removal of economic penalties, relaxation of overly restrictive operational practices, dealing with plant ageing effects, and resolution of outstanding safety analysis issues.

1. INTRODUCTION

1.1. Canadian regulatory philosophy

The current Canadian regulatory regime is based on the principle that the licensee has primary responsibility for safety and that detailed regulatory prescription is unnecessary and detrimental to the licensee carrying out that responsibility. The CNSC identifies, by publishing regulations, safety principles, high-level goals and standards; verifies licensees' performance against these and enforces compliance with the regulations. The interpretation of the high level requirements is left to the licensee. This leads to a licensing process with relatively little formal regulatory prescription, and significant latitude for licensees to choose the methods by which safety is ensured and demonstrated. This minimal prescription is particularly evident for safety analysis methods as there is very few formal rules set by the regulator. In demonstrating that the reactor design and operation meets the high-level requirements, a licensee is free to choose analysis methods, computer codes and quantitative derived acceptance criteria, which it considers to be appropriate, resource-efficient and supportable. The regulatory concurrence with the analysis methodology is being sought on a case-by-case basis.

1.2. CANDU reactor

The CANDU is a pressurised, heavy water moderated, and heavy water cooled, channel reactor. The first conceptual design of a CANDU-like reactor for electricity generation was produced by the end of 1957. The NPD reactor, connected to the grid in 1962, successfully operated for 25 years. There are currently 22 licensed CANDU reactors in Canada (8 of those are in laid-up state with 6 being prepared for restart). CANDU fuel is natural uranium which is contained within 28 or 37 element fuel bundles. The reactor core consists of a lattice of horizontal fuel channels within a calandria vessel, which contains the moderator. Re-fuelling is performed on power. The reactor is cooled by a heat transport (HT) system operating at about 10 MPa, which rejects heat to U-tube steam generators. The temperature of the heavy water coolant entering the reactor is in the range of 249–267^{o}C and the outlet header coolant temperature is limited by 293–310^{o}C (the higher values correspond to the newer CANDU designs). Two independent shutdown systems (SDS1 and SDS2) are poised to trip (shutdown) the reactor should any of the monitored plant trip parameters exceed their limits. Important safety systems that are designed to mitigate consequences of an accident or event are the "special safety systems" (SDS 1 and SDS 2, containment system, and emergency core cooling system); standby emergency systems (which include emergency electrical power, boiler emergency cooling and emergency service water); and process systems (for example, reactor regulating system, boiler auxiliary feedwater, primary circuit feed and bleed, and normal electrical power).

From a safety analysis perspective, the CANDU reactor has some distinctive features and characteristics:

- the natural uranium fuel resides in a matrix of individual horizontal fuel channels within short fuel bundles and is irradiated to relatively low burnups
- the primary circuit (heat transport system) is relatively complicated
- the moderator system is separate from the coolant, is at low pressure and temperature, and contains a significant amount of water
- re-fuelling is performed at power
- the reactor has a positive core void reactivity coefficient.

These design features historically have influenced formation of the Canadian regulatory philosophy, as well as of the safety analysis methods and acceptance criteria. For example, existence of a positive void reactivity coefficient led to a requirement of having two independent shutdown systems. As another example, because the fuel is contained within individual channels, rather than in an open lattice, concerns regarding the exothermic effects of fuel sheath oxidation are considerably reduced. Consequently, while there is a requirement to limit sheath temperature, a low limit (such as 1204 EC) is neither necessary nor imposed.

1.3. Safety analysis margins

Safety analysis does not provide safety (the latter is achieved through a robust design, high quality manufacturing and construction, and responsible operation). Safety analysis, however, allows to measure the safety of a nuclear reactor design and this measure plays a major role in any decision-making related to design, operation or licensing. The better safety is quantified the more informed decisions can be made.

The Probabilistic Safety Analysis offers one way to quantify the safety of an installation. When using the so-called deterministic safety analysis, which considers a

postulated set of transients and accidents, “safety margins” could be used as a quantitative measure.

The definition of a safety analysis margin for a selected acceptance criterion (e.g, the peak sheath temperature) can be written as:

safety analysis margin = acceptance criterion value — safety analysis prediction — [penalty for unresolved issues]

where the second term can be further specified in the following way:

safety analysis prediction = analysis centre value result + sum of biases + uncertainty at a specified percentile

A penalty for unresolved safety issues may be imposed, for example, in cases when the detrimental impact from an existing phenomenon is difficult to model accurately due to lack of reliable data.

In Canada, two types of acceptance criteria are used in safety analyses: radiological dose limits and derived acceptance criteria. The latter ones are usually significantly more restrictive than the dose limits. Considering a Large LOCA (LLOCA) event as an example, one such derived criterion will be maintenance of fuel channel integrity, which can be further subdivided by setting numerical limits for peak fuel and sheath temperature, number of ballooned pressure tubes, extent of fuel string axial expansion, etc. In practical terms, acceptance parameters (those which are compared with acceptance criteria) should be readily quantifiable in the safety analysis and it is for these parameters that margins are calculated.

It should be noted that in addition to the safety analysis margins other types of safety margins can be defined. For example, process parameter margin is the difference between the value at which the system is considered to be impaired and the nominal parameter value.

It is a firmly established principle in the Canadian regulatory practice to require that adequate safety margins be maintained and demonstrated by the safety analysis. The analysis must show that the facility meets all specified criteria with sufficient margins to cover any uncertainties in the methods of analysis. This is dictated by the need to have a “cushion” to accommodate new research findings, detrimental effects from ageing, unanalysed transients, unresolved safety issues and to allow certain flexibility for the operators. An alternative approach could be in incorporating sufficient margins directly in the acceptance criteria. However, this approach is perceived to be more restrictive.
.

2. LIMIT OF THE OPERATING ENVELOPE” SAFETY ANALYSIS

2.1. Elements of the limit of operating envelope analysis

CANDU reactors were historically licensed using deterministic conservative safety analysis, which evaluates consequences from postulated initiating events and sequences of events. This approach in the Canadian licensing practice is called the “Limit of the Operating Envelope” or LOE, method. The essential elements of the LOE analysis are as follows:

Analysis input parameters:
key (having significant impact on the analysis predictions) operating/design parameters:
Assumptions about operating parameters gave the name to this analysis approach. The values of all key-operating parameters are set simultaneously at the worst allowed values. Ageing effects are included in specifying input parameters. For each acceptance criterion (e.g. peak fuel temperature, peak sheath temperature, etc.) key input parameters are identified separately. It is recognized that setting all key operating parameters at their limits simultaneously may result in a un-physical reactor state (that is, a state which cannot exist due to dependencies between parameters). This is done to reduce the amount of analytical effort by avoiding the need for performing separate analyses for various combinations of parameters.

non-key operating/design parameters:
In most cases, no special treatment is specified for parameters that are seen as having small impact on the analysis predictions. In practice, design parameters are often set at their centre values while operating parameters — at their limiting values.

Modelling parameters:
Modelling parameters are set at their centre values while accounting for biases. As a rule, uncertainties are not included in the LOE analysis. This may be considered as not being in line with the strict interpretation of uncertainty accounting principles. Historically, the reasons for excluding random modelling uncertainties were as follows:

- large originally predicted margins
- belief that conservatism achieved by assuming the limiting values of operational parameters and imposition of certain deterministic assumptions more than adequately covers modelling uncertainties
- lack of well defined modelling uncertainties

The impact of modelling uncertainties is usually investigated by performing sensitivity studies.

Plant operating state:
A limiting operating mode (which most frequently, but not necessarily, is the full power operation) is analysed in detail to demonstrate compliance with applicable requirements. Other operating modes are analysed to the extent sufficient to show that they are bounded by the fully analysed operating mode. Availability and efficiency of the credited in analysis systems are assumed to be at the worst permissible levels. The limited-time but relatively frequent perturbations in the bounding operating mode, such as fuelling operations, operation with defected fuel, operation with minor equipment impairments, etc., can be assessed either through sensitivity cases or by imposing a penalty on the safety margin.

Deterministic assumptions:
A set of deterministic assumptions (such as crediting only the less efficient SDS out of the two fully capable shutdown systems, for example) is added to provide further confidence in the analysis findings, cover certain operational occurrences and add operational flexibility. All of these assumptions may not be detailed in regulatory documents but they have become firmly established in the licensing practice.

Computer models:
Best estimate codes are used whenever available; however, code validation is a long-standing requirement. Conservative models could be used for the sake of convenience or due to the lack of adequately validated models.

Utilities have long maintained that application of the LOE approach to safety analysis leads to unrealistically conservative predictions and has resulted, in some cases, in creation of a false perception of inadequately small safety margins. Below, a short description is given of a recent development, which highlighted difficulties in demonstrating safety margins while using the LOE approach.

2.2. Reactor physics code finding in the large LOCA analysis of CANDU reactors

As part of a study performed under a regulatory generic action item on replacement of reactor physics computer codes used in safety analysis, Ontario Power Generation (OPG) discovered non-conservatism in its old PPV/SMOKIN computational toolset. These computer codes have been used for the licensing LLOCA analysis for all of OPG's reactors. The discovered effect called into question the adequacy of the existing LLOCA analyses for all CANDU stations.

As pointed out earlier, one of the significant features of a CANDU reactor is a positive core void reactivity coefficient. In case of a LLOCA event this results in an over-power transient of approximately 2-second duration. The power pulse is terminated by the shutdown systems. Through analysis of this event with reactor physics, thermal-hydraulic and fuel computer codes, licensees must demonstrate that the LLOCA power pulse does not results in an unacceptable reactor response and, in particular, in loss of fuel channel integrity. For the LLOCA event, radiological doses to the public are also considered, but these are not limiting (predicted doses constitute approximately 5% of the dose limits).

When the over-power transient was analysed with a newer reactor physics toolset (WIMS/ CERBERUS) the predicted peak fuel bundle enthalpy was found to be approximately 15-20% larger than previously reported, which significantly reduced margins to acceptance criteria. All licensees have responded by imposing operational restrictions (for example, on the power levels, heat transport system and moderator isotopic purities, flux tilts, and additional requirements for overall SDS performance) to ensure that the peak fuel enthalpy predicted with these restrictions in place is less than or similar to that predicted in previously submitted licensing analysis. All licensees have submitted re-analyses of the LLOCA power pulse incorporating these changes.

The implemented operational constraints while allowing restoring safety margins have proved to be a substantial economic burden to utilities and a significant restriction of operating flexibility. A wide-ranging program with the objective to substantially improve safety margins has been launched, which includes:

- a variety of design changes
- experimental research
- application of a new, Best Estimate and Uncertainty Assessment (BE+UA) analysis methodology for LLOCA safety analysis

It should be noted that while this recent finding has stimulated efforts aimed at development and application of BE+UA methods, the work in this direction has started much

earlier and already been used in a variety of applications, for example, in development of Darlington Operational Parameter Methodology, CANDU 9 licensability assessment, licensing of the isotope production reactor MAPLE, albeit only as a supporting tool for the traditional LOE approach.

An additional and significant incentive for expeditious implementation of BE+UA methods in licensing is seen in providing an opportunity to address or alleviate certain currently unresolved safety analysis issues. The limiting accident transient conditions predicted in the LOE safety analysis led to substantial difficulties in adequate validation of models and codes for extreme values of temperature, pressure, radiation, etc. This resulted in gradual accumulation of outstanding safety issues, resolution of which usually requires costly experimental research under prototypical conditions. The traditional interim solution, while experimental evidence becomes available, would be to impose a penalty on the safety analysis to compensate for the potential effect due to an unresolved issue. In some cases, most notably for LLOCA, the available margins may no longer allow the use of such a remedy.

3. REGULATORY EXPECTATIONS FOR BEST ESTIMATE SAFETY ANALYSIS

3.1. Incentives for best estimate and uncertainty analysis

We can summarize now the reasons why the deterministic, conservative LOE approach is no longer seen by the Canadian licensees to be a completely suitable tool for safety analyses:

- in reality, the plant operates well away from the conservative analysis assumptions, and consequently, analysis predictions may not represent the real plant behaviour in the event of an accident
- even though it is recognized that potentially large “hidden” margins exist in addition to those demonstrated by conservative analyses, there is no means to quantify those margins
- in some instances, it is practically impossible or prohibitively expensive to validate the computer models for the range of parameters predicted in conservative analyses
- the extreme predicted accident conditions give rise to many safety analysis issues, resolution of which proves to be difficult and costly

On the other hand the BE+UA approach is gaining attractiveness because it:

- provides a more realistic prediction of plant behaviour during an accident, allowing at the same time to attain a predetermined confidence level in predictions
- facilitates resolution of many outstanding safety analysis issues by demonstration that accident consequences are more benign than previously predicted
- allows to narrow the range on parameters for computer code validation
- predicts the most likely behaviour of the plant in case of an accident which could be used for correct event diagnosis by plant operators
- potentially provides a means for incremental safety analysis with the use of past analysis results
- potentially, promises relaxation on certain operational restrictions and removal of penalties

CNSC staff has acknowledged [1, 2] that BE+UA analysis offer the potential for more realistic simulation of accident consequences and, thus, for resolving certain safety issues and relaxation of operational restrictions for utilities. It is also understood that the new methodology requires a substantial up-front effort in developing the methodology, collection of data, setting new compliance principles and reaching regulatory acceptance. It is perceived that the licensing application of BE+UA will be fraught with some specific difficulties, not encountered earlier. Recently, CNSC staff has undertook a project with the aim of identifying, in sufficient detail, of a set of "expectations" for best estimate analysis. Even though these "expectations" are not strict requirements, adherence to those should facilitate acceptance by the regulator of licensing submissions, which employ best estimate methods. The substance of these expectations is presented below.

3.2. Best estimate and uncertainty analysis expectations

CNSC staff "expectations" are described below as guidance for an analyst. They are based on the existing pertinent experience, both Canadian and international. These "expectations" are not formal requirements, however, it is assumed that the analyst would ensure that the BE+UA analysis performed for licensing purposes conforms with the intent of the "expectations".

3.2.1. Identification of the facility, event of interest, and acceptance criteria

To identify the facility, describe the following:

- specific facility design and location
- detailed composition of those facility systems and equipment which are credited in the analysis and impact significantly on the outcome of the analyzed event

To identify the analyzed event, specify the following:

- the initiating event and sequence of assumed failures
- plant operating mode prior to the initiating event
- initial state and assumed availability and performance of systems and equipment which are credited in the analysis
- any equipment and operator actions which are credited in the analysis
- rationale and criteria for selecting characteristics of the initiating event and event sequence for each of the applicable acceptance criteria

List all acceptance criteria and demonstrate that they address all threats posed by the analyzed event. Provide defendable justification for those acceptance criteria which are different from the dose limits and derived acceptance criteria identified in regulatory documents. In selecting acceptance criteria, ensure that properly validated models are available to demonstrate the conformance of acceptance parameters to the criteria.

3.2.2. Important phenomena and key parameters

To make the uncertainty assessment of the BE+UA safety analysis more resource efficient, the number of parameters whose uncertainties are accounted for explicitly, may need to be limited. Well-defined and stringent process should be applied to ensure that all important phenomena and parameters are identified and treated properly.

Identification of important phenomena

For each acceptance criterion, ensure that all important phenomena have been identified. Demonstrate, using validation results, that the important phenomena are adequately modeled in the computer codes, which are used in the analysis.

Ranking of input parameters

When identifying key input parameters, rank parameters separately for each acceptance criterion. Justify criteria and methods used to rank input parameters. In ranking, account for the uncertainty of a parameter as well as the sensitivity of the acceptance parameter to the input parameter uncertainty.

Treatment of high ranking parameters

Those input parameters which have been ranked high (key parameters) can be treated in two different ways in the BE+UA safety analysis, namely:

- statistically, when the uncertainty in an input parameter is propagated through the analysis
- conservatively, when the input parameter is set at a value which results in a conservative prediction of the output parameter. Use at least the 95th percentile at 95 percent confidence level as a conservative value for the key input parameters

Treatment of medium and low ranking parameters

Set the medium ranked input parameters (if such a category is used) at their conservative values. The low ranked parameters can be set at either limiting or design centre values, as by definition they have only negligible impact on the output parameters.

Confirmation of parameter ranking

Verify, upon the completion of the uncertainty assessment, that all key input parameters have been identified. Modify parameter ranking, if appropriate. Present evidence that the selected parameter ranking and their treatment are adequate based on the final analysis results.

3.2.3. Analytical tools

The analytical tools (i.e. computer codes, implementing models of phenomena occurring in the facility during the analyzed event) must satisfy certain criteria (described below) to be used in the BE+UA safety analysis

Applicability of codes

Establish the applicability of each code and the whole code suite for the analyzed facility and event by demonstration that the codes incorporate the following:

- models for all identified important plant systems and equipment
- models for all identified important phenomena
- accurate and stable numerical algorithms
- verified interface processes for data transfer between codes

Validation of computer codes

Provide evidence that codes have been validated over the range of conditions expected for the analyzed event. Identify, account for, and document scaling effects.

Produce a statement describing code accuracy for the intended application. For each code output parameter, which is either an input parameter for another code or an acceptance parameter, state the code accuracy for the range of conditions, including:

- the bias (systematic error) at the 95 percent confidence level
- the variance at the 95 percent confidence level.

For a negative bias to be credited in the analysis, demonstrate that it was quantified for the range of conditions typical for the considered event.

3.2.4. Deterministic assumptions

Traditionally, deterministic assumptions have been used in the analysis to allow for additional operational margins, introduce a degree of conservatism, account for modeling uncertainties, or to simplify the analysis. Certain deterministic assumptions have become firmly established as part of the design and licensing basis for the system concerned (for example, unavailability of shut-off rods with the highest worth; crediting only one SDS; treatment of the reactor regulating system response, etc.). Deterministic assumptions imposed on a specific analysis depend on the event analyzed.

Identification of deterministic assumptions

Identify all deterministic assumptions in the analysis. Demonstrate that the regulatory requirements applicable to analysis assumptions have been met. Identify and justify deviations from the established licensing practice. Any relaxation of the assumptions, previously accepted in the licensing analysis, must be rationalized based on the operational experience and experimental evidence. The regulatory principles such as “defense in depth”, etc. should be maintained.

Initiating event

Even though the plant state prior to a failure and subsequent transient behaviour can be treated in the BE+UA analysis using statistical distributions of operational and design parameters, select the initiating event which would be bounding for each of the applicable acceptance criteria, e.g. in a LLOCA analysis select the break location, type and size based not on probabilistic arguments, but such that they would maximize the consequences.

Interim limitations

Until the BE+UA safety analysis methods are found by CNSC staff as being firmly established more restrictive, deterministic assumptions may be imposed on the analysis to compensate for the lack of experience with licensing applications of such methods. As these methods gain the regulatory acceptance, the deterministic assumptions could be reassessed.

3.2.5. Analysis input parameters

Prior to the analysis, identify and list all operational, design and modeling parameters needed for the analysis.

Operational and design data collection

Describe processes used at the facility for collecting data characterizing operational and design parameters. In collecting operational data, specify to which operating state they correspond.

Establish criteria for the data sample size, needed to determine, with a pre-defined confidence level, the parameter mean, standard deviation and type of the distribution. Justify data collection frequency, needed to capture different modes of operation including infrequent events such as equipment/system malfunction and failures.

Identify operational and design data variability ranges and the data measurement or prediction errors. Provide references to records documenting data.

Covariances and trends in operational data

Test data to identify covariance and its underlying causes. Where covariance exists, ensure that the parameters' interdependence is treated appropriately in the analysis.

Demonstrate that the data collection processes allow identification of trends in operational data behaviour, in particular, of the ageing effects.

Pooling of operational data

For the data from multiple units or similar facilities to be admissible in the BE+UA analysis of a particular facility, demonstrate that there are no systematic differences in design or operating procedures, which could affect the analyzed event. Data pooling should not be done if there are statistically significant differences in plant behaviour.

Plant operating states

In the analysis use only operational data applicable to the plant operating state which is being analyzed.

Qualification of modeling parameters

Provide sufficient evidence to support selected values of modeling parameters for the range of conditions characteristic for the analyzed event. Identify and justify all instances when modeling parameters must be applied beyond the range of conditions for which reliable data exists.

3.2.6. Quantification of uncertainties

When performing the BE+UA analysis, uncertainties of the input operational and design parameters and of applied models, need to be reliably established. Knowing parameter

uncertainty is a prerequisite for parameter ranking and performing the integrated uncertainty assessment.

Sources of parameter uncertainties

In quantifying operational parameter uncertainty account for the following contributors:

- operational variability
- trends
- measurement errors
- instrument drift
- calculation errors, etc.

In quantifying design parameter uncertainty account for the following contributors:

- design allowances
- fabrication tolerances
- measurement errors
- test and calibration accuracy, etc.

In quantifying modeling uncertainties account for the following contributors:

- effects arising from validation of a model under non-prototypic conditions
- scaling effects
- unmodeled processes
- data libraries
- simplifications
- nodalization effects
- accuracy of numerical solution schemes, etc.

Uncertainty characteristics

To adequately characterize the uncertainty of a parameter:

- select the distribution function conservatively enveloping measurement or test data
- quantify the distribution function parameters (i.e. the range of variance for a uniform distribution function, mean and standard deviation for a normal distribution)
- identify systematic error (bias) where applicable

In specifying uncertainty characteristics (mean, variance, bias, ranges, etc.) for the purposes of uncertainty assessment in the BE+UA safety analysis, use values defined at least at their 95 percent confidence level in the conservative direction.

3.2.7. Integrated uncertainty assessment

The objective of integrated uncertainty assessment in the BE+UA analysis is to generate the uncertainty distributions for output parameters of interest, i.e. acceptance parameters. In other words, the integrated uncertainty assessment allows to determine probabilities of meeting specified acceptance criteria under postulated accident conditions.

Surrogate tools

Implement stringent criteria to demonstrate that surrogate analytical methods replacing detailed and validated computer codes, are admissible in uncertainty assessment. In particular,

quantify and minimize the additional uncertainty introduced by the application of surrogates, and account for it as an additional source of modeling uncertainty.

Distribution tails

In generating statistical distributions of output parameters employ procedures ensuring that tails of input parameter distributions (i.e. low probability values) are appropriately included.

Acceptance parameter percentile

In judging conformance with the acceptance criteria, use at least 95th percentile of the acceptance parameter distribution at 95 percent confidence level. For events with a relatively higher probability of occurrence, a higher percentile may be more appropriate (seek agreement with CNSC staff on the percentile to be used for demonstration of conformance prior to the analysis).

Present results of the acceptance parameter calculation as statistical distributions so that inferences can be made about probabilities of exceeding various limits and existence of cliff-edge effects.

Confirmation of parameter ranking

An important element of uncertainty assessment is confirmation of acceptance parameter sensitivities to uncertainties in input parameters. Demonstrate, by performing sensitivity studies, that all key input parameters that significantly influence acceptance parameter behaviour have been identified.

3.2.8. Expert judgment

Use of judgement should be minimized to the extent practicable. However, under lack of definitive information, expert judgement can be utilized to rank phenomena and parameters, assign bounding values, select probability distribution functions, etc. To improve confidence in such judgements, explicit rules for soliciting expert opinions should be applied.

Rules for expert judgement

Establish rules for use of expert judgement. These rules should ensure scrutable process and address the following:

- identification of areas where expert opinions are needed and admissible
- requirements to experts' qualification and to the number of experts
- application of a formal approach for soliciting and integration of judgements
- referencing of supporting information
- documentation of experts' recommendations.

Confirmation of expert judgement

Verify expert judgement in case when a posteriori confirmation of judgement is possible (e.g. assumed sensitivities to input parameters, selection of key parameters, etc).

3.2.9. Validity of the analysis

The BE+UA analysis relies on facility-specific operational and design data. Design modifications and operational procedure changes alter the way the plant operates and, consequently, the way the plant responds to an accident.

Plant states bounded by analysis

Identify all plant states, which are not explicitly bounded by the analysis. Perform separate assessments addressing those states to demonstrate that the applicable acceptance criteria (which may be different depending on the plant state) are met.

Deliberate operation away from "operating centre"

There is an important distinction between stochastic variation in plant operating parameters and deliberate operation away from the historical operating centre values of parameters, e.g, due to an impairment or failure of equipment. If such a deviation is not in demonstrably safe direction (but within allowable limits) then operational procedures should exist to return the plant operating parameters back to the operating centre, within a specified time. If the time of operation away from operating centre is statistically significant then such states should be analyzed separately.

Trends in plant parameters

Provide evidence that adequate processes are in place to collect, monitor and evaluate the key plant parameters so that trends in parameter behaviour can be captured, understood and accounted for in the analysis.

Compliance of plant operation to analysis assumptions

Establish operational compliance for key plant parameters that ensures that plant operation is consistent with the analysis assumptions. Explicitly address the issue of maintaining statistical distributions of key parameters assumed in the analysis. Specify the extent to which the analysis relies upon operational compliance.

Analysis "Shelf life"

Identify criteria to judge the analysis validity when parameter variation characteristics change from those assumed in the analysis. Establish a process to periodically confirm that these criteria are met.

3.2.10. Non-typical plant states

The BE+UA analysis by definition focuses on the most likely state, conditions, responses and behaviour of a facility and its components. It is important, therefore, to ensure that facility states not covered by the BE+UA analysis are considered and their safety implications recognized and evaluated.

Assessment of non-typical plant states

Perform assessments that consider the initial plant operational conditions, equipment availability, system responses that are not typical but allowed by operating procedures. Examples of such states are:

- reactor upsets
- failures of equipment
- operation with defected fuel
- fuelling operations
- shim operation
- startup/shutdown process, etc.

Same acceptance criteria should be applied as identified for the BE+UA analysis or any alternative requirements should be adequately justified.

4. EXAMPLE OF AN APPLICATION OF THE BE+UA ANALYSIS

As was mentioned previously, the industry puts a lot of faith in demonstration of improved safety margins with BE+UA methods. Ontario Power Generation (OPG), the largest utility in Canada, has recently performed and formally presented to the CNSC the first submission where the best estimate analysis was used as an integral part for demonstration of adequate safety margins (reference 3 provides more detail of this application). In order to address the issue of trip coverage for the single HT pump trip event for Darlington NGS and to support return to the full power operation (currently Darlington operation is limited to 98% full power), Ontario Power Generation proposed certain design changes to the shutdown systems. The changes involve improvements to the primary Heat Transport Low Flow (HTLF) trip, and the installation of a new backup Reactor outlet header-to-Reactor outlet header Differential Pressure (RRDP) trip. The primary trip is intended to prevent the fuel sheath dry out in the limiting fuel channel if a single pump trip occurs. The backup trip is designed to prevent the fuel sheath temperature from attaining or exceeding 600^{o}C during a single pump trip event.

Conventional LOE safety analysis predicts little or no margin between the initiation of the HTLF trip and the occurrence of fuel sheath dry out for the single HT pump trip event. For the RRDP trip, the LOE analysis predicts that the fuel sheath temperature would slightly exceed the 600^{o}C limit prior to trip initiation. The purpose of the best estimate and uncertainty analysis was to demonstrate that comfortable margins exist for both safety criteria, at the 95% probability level, and at 95% confidence. Following a HT pump trip, the coolant flow in the affected loop begins to run down, causing critical heat flux (CHF) conditions and subsequent dry out to first occur in the limiting fuel channel. Through application of the parameter ranking process, several key parameters were identified as important in determining the thermal-hydraulic response of the HT system and the limiting fuel channel, following a single HT pump trip. They are: bulk reactor power, reactor inlet header temperature, reactor outlet header pressure, limiting channel power, reactor power tilt, HT system liquid relief valve (LRV) pressure set point, fuel bundle and bundle element power at the peak power in the limiting channel, fuel burn up, fuel sheath-to-coolant heat transfer coefficient, and CHF. The operating or experimental data relevant to these parameters have been assessed, and corresponding probability distributions have been estimated.

The results of the BE+AU analysis [3] show that the HTLF trip (primary trip) has a 95/95 margin of 1.57 seconds prior to the occurrence of fuel sheath dryout. For the backup

trip, a similar percentile and confidence level calculation yielded that the RRDP trip has a 95/95 margin of at least 9.30 seconds prior to the occurrence of 600^{o}C fuel sheath temperature. CNSC staff has reviewed this analysis and raised a number of issues, which are being addressed by the utility.

Using lessons learned during this rather limited-scope project, OPG is currently carrying out a more extensive analysis of a LLOCA event for Darlington NGS. Another licensee, Bruce Power, has also indicated their intention to conduct a BE+UA analysis of a LLOCA event for Bruce NGS. For Bruce units, which currently operate at 90% full power, the best estimate analysis is one of several initiatives aiming at improving safety margins (other activities involve extensive design changes) and, potentially, increasing the allowed power level. AECL, the designer of CANDU-6 units, is similarly involved in development of a best estimate methodology; its prototype application was reported, for example, in [4]. There is close cooperation between licensees in developing of the methodology and rules for its application. The focus of effort is on the LLOCA analysis — because of the recent reactor physics code finding as well as due to existence of several unresolved issues with the LLOCA LOE analysis.

5. CONCLUSION

This paper presents a regulatory view on the reasons, incentives and expectations related to development and application of the best estimate and uncertainty assessment safety analysis methodology in Canada. Even though the efforts by utilities has not yet resulted in any completely successful licensing BE+UA application, there is confidence that the best estimate methods will find wide use in the licensing process in Canada in the not-so-far future. It is believed that following a substantial, initial up-front investment in the development of the methodology and establishing processes for collection and qualification of data, the subsequent effort for performing BE+UA analyses will not be significantly larger than for the traditional conservative analysis. Results of the BE+UA analysis are expected to play an important role in decisions related to removal of economic penalties, relaxation of overly restrictive operational practices, dealing with plant ageing effects, and resolution of outstanding safety analysis issues.

ACKNOWLEDGEMENTS

The author would like to express his appreciation for input, ideas and comments from Dave Newland, Haldun Tezel, Jeet Khosla and other CNSC staff.

REFERENCES

[1] NEWLAND, D.B., “The Developing Roles of “Best-estimate” Thermal-Hydraulic Calculations and Uncertainty Analyses in Licensing in Canada”, OECD/CSNI Seminar of Best-Estimate Methods in Thermal Hydraulic Safety Analysis, Ankara, Turkey, June 1998.

[2] NEWLAND, D.B., TEZEL, H.O., “The Transition to Best-Estimate Analysis: A Regulatory Perspective”, in Proceedings of ANS International Meeting on Best Estimate Methods in Nuclear Installations Safety Analysis”, Washington, DC, November 2000.

[3] LUXAT, J.C., HUGET, R.G., LAU, D.K., TRAN, F., “Development and Application of Ontario Power Generation’s Best Estimate Nuclear Safety Analysis Methodology”, in Proceedings of ANS International Meeting on Best Estimate Methods in Nuclear Installations Safety Analysis” Washington, DC, November 2000.
[4] SILLS, H.E., ABDUL-RAZZAK, A., DUFFY, R.B., POPOV, N., “Best Estimate Methods for Safety Margin Assessment”, in Proceedings of ANS International Meeting on Best Estimate Methods in Nuclear Installations Safety Analysis”, Washington, DC, November 2000.

ABBREVIATIONS

AEAW	Atomic Energy Authority Winfrith
ATHLET	analyses of thermalhydraulics in leaks and transients
ATWS	anticipated transient without scram
BE	best estimate
BIC	boundary and initial conditions
BWR	boiling water reactor
CDF	core damage frequency
CIAU	code with capability of internal assessment of uncertainty
CSAU	code scaling, applicability and uncertainty
CSNI	Committee on the Safety of Nuclear Installations
DA	deterministic analysis
DBA	design basis accident
DNBR	departure from nucleate boiling ratio
ECCS	emergency core cooling system
ENUSA	Empresa Nacional del Uranio, SA
GE	General Electric
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit
IJS	Institut "Jožef Stefan"
ISP	international standard problem
ISPN	Institut de Protection et de Sûreté Nucléaire
ITF	integral test facility
LBLOCA	large break loss of coolant accident
LOCA	loss of coolant accident
LOFA	loss of flow accident
LSTF	large scale test facility
MOX	mixed oxide
NPP	nuclear power plant
PIE	postulated initiating event
PSA	probabilistic safety analysis
PSC	probabilistic safety criteria
PWR	pressurized water reactor
QA	quality assurance
RCS	reactor coolant system
RELAP	reactor excursion and leak analysis program
R-Y	Reactor-Year
SAR	safety analysis report
SBLOCA	small break loss of coolant accident
SET	separate effects test
SPDS	safety parameter display system
UA	uncertainty analysis
WWER	Voda-Vodianoj Energeticheskij Reaktor

CONTRIBUTORS TO DRAFTING AND REVIEW

Antila, M.	Fortum Nuclear Services Ltd, Finland
Dusic, M.	International Atomic Energy Agency
Fil, N.	EDO Gidropress, Russian Federation
Glaeser, H.	GRS, mbH, Germany
Hajra, P.	Atomic Energy Regulatory Board, India
Hortal, J.	Nuclear Safety Council, Spain
Mandowara, S.L.	Nuclear Power Corporation of India Ltd, India
Misak, J.	International Atomic Energy Agency
Nemes, I.	Paks Power Nuclear Plant Ltd, Hungary
Polyakov, A.	South Ukrainian NPP, Ukraine
Prosek, A.	Jozef Stefan Institute, Slovenia
Rimkevicius, S.	Lithuanian Energy Institute, Lithuania
Stanev, I.	Energoproekt, Bulgaria
Tkac, A.	Engineering Design and Research Organization, Slovakia
Victorov, A.	Canadian Nuclear Safety Commission, Canada
Vymazal, P.	NPP Dukovany, Czech Republic
Wellens, B.	Tractebel Energy Engineering, Belgium