NATIONAL NUCLEAR REGULATOR

REQUIREMENTS DOCUMENT

No.	Title	Rev.
RD-0016	**Requirements for authorisation submissions involving computer software and evaluation models for safety calculations**	0

APPROVED: ____________________ DATE: 25/04/06

CHIEF EXECUTIVE OFFICER

Table of contents

1. INTRODUCTION 3

2. DEFINITIONS 4

3. SCOPE 6

4. MAIN ELEMENTS OF EVALUATION MODEL/SOFTWARE VALIDATION 7

4.1. Verification and Validation 7

4.1.1. Physical Processes 7
4.1.2. Physical Modelling 7
4.1.3. Solution of Equations 8
4.1.4. Correlations 8
4.1.5. Comparison with Experiment 9
4.1.6. Comparison with Plant Data 10
4.1.7. Comparison with Analytical Solutions 11
4.1.8. Comparison with Alternative Calculation Methods 11
4.1.9. Biased Calculations 12
4.1.10. Best Estimate Calculations 13

4.2. Assurance of Quality 13

4.2.1. Computer software quality assurance 14
4.2.2. Data quality assurance 15
4.2.3. User Proficiency 15

5. REQUIREMENTS FOR LICENSING STAGES 16

5.1. Stage 1: Acceptance of Concept Safety Case 16

5.2. Stage 2: Construction and Installation 17

5.3. Stage 3: Fuel on Site, Fuel Loading, Testing and Commissioning 19

5.4. Stage 4: Plant Operation 19

6. REFERENCES 19

1. INTRODUCTION

Analysis of plant design and operation using computer software forms an important part of a modern safety case. Clearly the question of software validation and verification must therefore be addressed. Although computer software programs are the main calculation method employed in nuclear plant design and analysis, occasionally calculations by hand are performed. The verification and validation procedures described here are equally applicable to either route. Unless otherwise stated references to calculation methods may be taken to encompass both computer software and calculation procedures carried out by hand. For the purpose of this document spreadsheets and similar calculations tools shall be considered in the same manner as other Commercial Off The Shelf (COTS) software.

This Requirements Document contains and details the requirements of the National Nuclear Regulator (hereafter referred to as the NNR) that must be met by applicant and designer. Each requirement is identified by a unique number in brackets.

The NNR will not provide a general approval for specific computer software irrespective of its intended use, but will only state its acceptance for specific applications in the safety analysis under specific conditions. For specific applications also an independent assessment involving separate calculation models and software programs may be required.

Guidance to support all of the requirements stated in this document in terms of Power Reactors is given in NNR LG-1045 /1/.

2. DEFINITIONS

Term	Definition
Alternative Calculation	A Calculation that is made with alternative methods to verify correctness of another original Calculation.
Alternative Calculation Method	A Calculation Method that is developed with alternative and independently developed methods to verify correctness of another original Calculation Method.
Calculation	Manual or computer computation used for design, analysis, or to demonstrate the adequacy of a design. The term Calculation may also be used to describe a series of Calculations performed using variations to the inputs, Model parameters, etc.
Calculation Method	The methodology used to perform a calculation. The term Calculation Method refers to the model, software, data or manual approach used.
Calculation Model	An analytical representation or quantification of a real system and ways in which phenomena occur within that system, used to predict or assess the behaviour of the real system under specified conditions. Where a Software Product is used the Calculation Model is the combination of the System Model and Software Product.
Evaluation Model	A calculation framework consisting of **one or more** Calculation Models and specific inputs used to model specific system behaviour under certain conditions and linked to specific Safety Case assessment(s) and/or objective(s).
Integral Effects Test	Tests designed to enable most of the phenomena of interest to the reactor plant situation to occur with interaction between them.
Mitigation Measure	Approach, justified in detail in the license submission, which is taken to address a source of weakness in the available validation evidence needed to support a Calculation or Method for use in the Safety Case.
Model	A representation of a real world process, device or concept.
Separate Effects Test	Tests designed to examine at the most a few phenomena which the calculation is attempting to model
Software	Computer program or script.

Software Product	The set of computer programs, procedures, and possibly associated documentation and data.
System Model	The inputs to a Software Product representing the physical properties of a real system. A System Model comprises the spatial and/or temporal model of the system to be analysed and the associated sets of input data.
System Model data Validation	The evidence supporting the System Model data that demonstrates that the achieved calculation using the data is fit for its purpose when applied Mitigation Measures are also taken into account.
Validation (except regarding System Model data)	The evidence that demonstrates that the calculation method is fit for its purpose. When calculating physical processes it may mean showing that the calculation is bounding with a suitable degree of confidence rather than a best estimate.
Verification	The process of ensuring that the controlling physical equations have been correctly translated into software coding, or in the case of hand calculations, correctly incorporated into the calculation procedure. For the purposes of this document verification is taken to be part of the validation submission.

3. SCOPE

This document is intended to apply mainly to the assessment of the verification and validation of important physics and engineering analysis software and calculation methods used within the safety design basis. In exceptional cases alternatives to specific requirements of this document may be used when authorized by the NNR. A respective justification has to be submitted before such an authorization can be granted.

Calculations of severe accident conditions may involve the predictions of extreme physical behaviour and the calculation methods used are often not so amenable to rigorous validation. Nevertheless, any validation submissions for severe accident calculation methods should conform in a general way to the requirements given in this document.

<u>This document is not applicable to the assessment of software used for protection and control in operation.</u>

Principal Requirements Summary

(1) Information about computer software and evaluation models for safety calculations must be comprehensive.

(2) The submission must demonstrate that all models used are robust and have been benchmarked directly or indirectly against experimental data.[1]

(3) The licensee must provide for NNR review, a complete description of each evaluation model which is sufficient to permit technical review of the analytical approach, empirical correlations, the equations used, their approximations in difference form, the assumptions made and included in the software products, procedure for treating software input and output information, including specification of those portions of the analysis performed both with and without using software products, values of parameters, and all other information necessary to specify the calculation procedure.

(4) Solution convergence must be demonstrated for each calculation, by studies of system modelling or nodalisation and calculation time steps.[2]

(5) Sensitivity studies must be performed for each evaluation model, to evaluate the effect on the calculated results of variations in nodalisation, time step size and phenomena assumed in the calculation to predominate. For items for which results are shown to be sensitive, the choices made must be justified.

(6) The empirical models and correlations used in the evaluation model must be compared with relevant data. Predictions of the entire evaluation model must be compared with applicable experimental information. If an evaluation model for evaluating the behaviour of the plant system during a postulated accident includes one or more computer programs and other information, overall program behaviour must be checked against results from standard problems or benchmarks.

[1] An indirect benchmark in this sense would be a comparison with an alternate software product which itself is benchmarked against experimental data.

[2] Solution convergence may be influenced by multiple solutions or by discontinuities of physical properties.

4. MAIN ELEMENTS OF EVALUATION MODEL/SOFTWARE VALIDATION

In the assessment of the computer software verification and validation submissions, the NNR needs to be satisfied in a number of general areas as explained below. The extent of that satisfaction depends upon the importance of the software to the safety case, the complexity and level of understanding of the phenomena and processes involved, and the degree of extrapolation from experiment or practical experience to the situation being modelled.

The following section lists a number of areas that the NNR would expect to form the main elements of a verification and validation package, although the requirements will vary depending on the structure of the method and its application. For instance software used to carry out fault tree analysis does not model physical processes and would require consideration of only a limited number of the areas below.

The areas that are expected to form the main elements of software product and, more generally, calculation method verification and validation are discussed in the sub-sections below.

4.1. Verification and Validation

4.1.1. Physical Processes

Calculation methods are often developed to apply to a limited range of plant states. For instance different calculation methods are frequently used to model steady state operations and transient operations.

Similarly, in analysing a particular fault situation, different calculation methods may be used for different phases of the fault. In these situations, the calculation method may have been developed to model a definable range of physical phenomena and will not be applicable outside that range. The limits of applicability are often based on an identifiable change in the dominant physical processes which are predicted to take place.

(7) The submission must indicate the dominant physical processes that are expected to occur in each calculation method and define the limits of application of these calculation methods.

(8) The validation submission must define the physical processes, which the calculation method is designed to model.

(9) The validation submission must identify all changes in the physical processes, which make the method no longer applicable.

4.1.2. Physical Modelling

Modelling a physical situation requires the development of mathematical equations to describe the processes that are believed to occur. In general a number of idealisations and simplifications are applied to enable a tractable mathematical formulation to be made. For instance, complex 3-dimensional geometry may be reduced to a simplified 1- or 2-dimensional approximation.

(10) In describing the equations used to represent the various physical processes which occur during the fault condition the derivation of the equations must be clearly stated along with the justification for any simplifying assumptions.

(11) The submission must enable the assessor to follow the derivation of the controlling equations.

4.1.3. Solution of Equations

The solution of the controlling equations usually requires numerical approximation techniques, for instance, finite differences, finite elements or Monte-Carlo methods.

(12) The submission must justify the solution methods employed.

(13) The submission must demonstrate the accuracy of these solution methods.

(14) The submission must justify the numerical approximation methods used in the solution of equations.

(15) The submission must demonstrate sufficient accuracy from the numerical approximations.

(16) Significant numerical problems that can occur with particular numerical approximation techniques must be listed along with an explanation as to why they will not invalidate the calculations for which the method may be used.

(17) The calculation must check that any basic conservation laws, such as for mass or energy, are indeed conserved by the numerical scheme employed.

(18) There must be a demonstration that the nodalisation used is fine enough to provide a converged solution.

(19) Where a nodalisation fine enough to provide a converged solution is not practicable, the submission must explain why any lack of convergence does not invalidate the relevant safety argument(s).

4.1.4. Correlations

In many cases the physical complexity of the process being modelled means that a physically based mathematical description cannot be derived. In these cases empirical correlations may be used to represent the essential parts of the physical process and so enable the model of the problem to be 'closed'.

For non-trivial correlations the implementation should be clarified by showing how the correlation is implemented in the calculation using a flow chart or by other analogous means.

(20) For each correlation used the submission must make a statement on:

- (i) Claimed accuracy
- (ii) Range over which the correlation applies
- (iii) Methods to prevent use outside this range
- (iv) Relevance of the database to the transient or steady state scenarios in which the correlation is used.

(21) The accuracy of the fits of correlations to the data base must be shown in the submission by graphs or by analogous means.

(22) The validation submission must provide the technical basis and justification for the use of each correlation in the range of interest to safety case calculations.

(23) It must be explained what steps are taken to prevent the correlation being used outside that range. The important correlation parameters must be stated along with the correlation range for each of them.

(24) If a correlation is being used outside the range justified by its database, the submission must provide an assessment of the effects on the accuracy of the calculation results.

(25) When correlations are derived from experiments in scaled-down facilities the validity of extrapolating their use to the full sized plant must be demonstrated.

(26) The empiricism built into the correlation must be derived from a wide enough database to ensure applicability to all anticipated plant conditions for which the correlation is being applied.

(27) If correlations are used in the calculation that do not cover the anticipated plant conditions being analysed, this use must be justified.

(28) Where the calculation switches between different correlation ranges or between separate correlations, discontinuities are often introduced. Any modifications required to overcome such computational difficulties must be described.

4.1.5. Comparison with Experiment

Having demonstrated the mathematical modelling required in a calculation, the combined effect of the elements of that modelling needs to be tested. One way of gaining calculation validation evidence is by analysing experiments and comparing the predictions of the software (or other calculation tool) against the experimental results. These experiments must be as well instrumented as practicable so that as much as possible is known about the conditions being studied.

A range of tests enables the ability of the relevant software or other calculation models to extrapolate from one situation to another to be determined. This is of particular importance since often the plant fault conditions cannot be simulated by experiment.

Experimental comparisons tend to be of two types:

- 'separate effects tests' (SET) designed to examine at the most a few phenomena which the calculation is attempting to model,
- 'integral effects tests' (IET) designed to enable most of the phenomena of interest to the plant situation to occur with interaction between them.

Both types of tests can be carried out at various scales but integral effects tests are usually limited to fairly small scales by considerations of cost and complexity and will typically provide only very limited validation evidence for particular models. Thus both types of test should be used as far as possible to validate the predictive capabilities of the computational method. Wherever possible, comparisons should be made with integral experiments at a range of scales.

Many calculation methods are 'tuned' to a greater or lesser degree to results from a specific experimental facility. Tuning is the process of recalculating the same test case with adjustments, for example, in input parameters, user options or nodalisation until the best possible agreement is obtained. A calculation method that has been gradually tuned to a succession of slightly differing test cases may show excellent agreement with results from a particular facility but this does not necessarily indicate its predictive ability elsewhere.

A 'pre-test' calculation is carried out prior to the test being done and has to assume appropriate test starting and boundary conditions. A 'blind' calculation is usually carried out after the test and will employ starting and boundary data from the actual test. A 'double-blind' calculation is a more restricted blind calculation on a facility for which the user has no prior modelling experience. Such calculations are also of benefit in assessing and/or developing analyst experience.

(29) For comparison of software products and/or calculation models against experiment a range of well instrumented experiments are required, starting with simple representations and leading to more complex situations which try to represent the actual conditions experienced. Otherwise a justification must be presented giving the reasons that such a range is not necessary or can be otherwise limited in extent.

(30) The experiments must be conducted at :

- (i) a scale close to the intended application or
- (ii) at a range of scales to allow the appropriate scaling factor methodology and values to be determined or
- (iii) a robust justification must presented to specify why the adopted scale is satisfactory for the method under consideration.

(31) The validation submission must comprise an assessment showing that the applied experiments provide information which is significant for the validation of the respective calculation method.

(32) Justification for the exclusion of any experiments, which seem particularly relevant must be presented in the submission.

(33) When analysing separate effects tests, the correlations that are being tested must be identified and reference to the accuracy claimed in section 4.1.4 above must be made.

(34) A distinction must be drawn between any database that was used to develop the correlations and that which is being used as input data for the validation exercise itself.

(35) The ability of the calculation method to extrapolate from small scale tests to the plant situation must be discussed in relation to integral experiments.

(36) The validation submission must include comparison calculations for a range of different facilities or robust justification for the absence of such a range must be presented.

4.1.6. Comparison with Plant Data

Whenever possible, calculation predictions should be compared with actual plant data.

Tests carried out in full sized plants during commissioning or start-up procedures, as well as operational transients or accidents, can be a useful source of data and should, where possible, be included in the validation submission. In general plants are not as well instrumented as specially designed experiments and measurements taken from them may be too coarse to allow quantification of calculation accuracy. Such data may however be used to check the validity of computed trends as the boundary or initial conditions are parametrically varied.

Plant tests normally do not provide the physical conditions that occur in more severe transients and consequently any conclusions based on plant data comparisons should be drawn very carefully for such areas.

(37) Any plant data comparisons included to provide calculation validation evidence must be documented in detail. This must include detailed descriptions of data uncertainties and calculation uncertainties in particular.

4.1.7. Comparison with Analytical Solutions

Where appropriate the submission should compare calculations with analytical solutions to benchmark problems.

Certain well-defined problems may have established analytical or numerical solutions. Also asymptotic analytical solutions may be available for limiting cases. In the areas of structural mechanics and neutron physics for instance, numerical 'benchmark' problems already have a long tradition. However, the use of numerical benchmark problems will provide information on the mathematical solution ability of the calculation method rather than on the physical modelling and consequently their value for validation may be limited.

Nonetheless it is important to ensure that numerical solution errors are small compared with modelling errors and benchmark problems may be a way of establishing bounds on these errors, albeit for limited types of problems.

(38) Where numerical benchmark problems are included in the submission these must fulfil the following requirements:

- (i) the model equations must represent a well-posed mathematical problem with a unique solution;
- (ii) every term in the equations must be defined and written down explicitly and
- (iii) the initial and boundary conditions must be defined explicitly.

Although these requirements limit the types of problem that can be considered, a validation submission should incorporate such comparisons.

(39) If numerical benchmark problems are not included in a validation submission, it must be explained why it is not appropriate to do so.

4.1.8. Comparison with Alternative Calculation Methods

The validation submission should, if possible, compare calculations carried out with the safety case calculation method against those obtained using alternative, independently developed methods.

In addition to comparing the calculations with experiment, useful information can be obtained by comparing one calculation method against another. Clearly comparison with a calculation method which is a derivative of, or very similar to that used in the safety case would not necessarily yield useful results.

When the safety case is based on a proprietary software product then comparisons should preferably be made with non-proprietary software products, as these will have generally been subject to more wide-ranging scrutiny and use.

If the safety case is made with a calculation method that contains gross simplifications then, where possible, more advanced methods should be used in the comparison to demonstrate that the simpler method is taking adequate consideration of the dominant physical phenomena.

(40) The alternative calculation method must have been developed independently of that used in the safety case and must be sufficiently different from it in either numerical methods or physical modelling to make the comparison worthwhile.

(41) The alternative calculation method used for comparison must include or reference a statement about its validation, since comparisons against a demonstrably unreliable calculation would be pointless.

4.1.9. Biased Calculations

Uncertainties in the representation of important physical processes may be such that pessimistic models of these processes are deliberately built into the calculation procedure.

Unless otherwise stated, conservatism shall mean that the calculated relevant safety parameters (e.g. temperature, pressure, radiation field, strain, etc.) are biased on the conservative side throughout the calculation for the whole spectrum of operational or fault conditions modelled.

The validation of biased methods against experiment can raise particular difficulties, since the pessimism may introduce features into the calculations, which do not correspond with what is seen in the test. In order to make meaningful comparisons with experiment, sensitivity studies may be necessary, in which calculations are made with any deliberately pessimistic bias removed from relevant parts of the modelling.

(42) If the calculation method is to be used to make a pessimistically biased calculation, the conservatism associated with each assumed pessimism, must be demonstrated.

(43) Any claim to conservatism in calculation methods with deliberately built in pessimistic models of physical processes must be justified.

4.1.10. Best Estimate Calculations

A best-estimate calculation employs modelling that attempts to describe realistically the physical processes occurring in the plant.

Deriving the overall uncertainty for a best-estimate calculation method may be a difficult undertaking. The combined uncertainty from all the individual models within the procedure is not necessarily the total uncertainty for the calculation. Uncertainties also come from applying models derived from small scale experiments to the full-sized plant (scaling uncertainties) as well as from the uncertainties associated with the input boundary and initial conditions.

For complex calculation methods a rigorous derivation of an uncertainty 'response function' (i.e. the response of the calculation to arbitrary uncertainty variations in the constituent models) would usually involve excessive numbers of sensitivity studies and alternative approaches will generally involve judgement of which 'dominant phenomena or 'key models' need to be considered.

(44) When a calculation method is used to make unbiased or best-estimate calculations the validation submission must present a detailed derivation of the uncertainty bounds to be associated with important results.

(45) The modelling must provide a realistic calculation of any particular phenomenon to a degree of accuracy compatible with the current state of knowledge of that phenomenon.

(46) The neglect or simplification of any phenomenon must not be treated by including a deliberate pessimism or bias, but must form part of an assessment of the overall modelling uncertainty.

(47) In arriving at the overall calculational uncertainty all sources of uncertainty including scaling uncertainties and uncertainties associated with initial and boundary conditions must be taken into account.

(48) The methodology used to combine the various sources of calculation uncertainty must be described and justified.

(49) Judgements concerning dominant phenomena and key models must be clearly stated and justified.

(50) For each parameter, which is judged to be of particular significance to the derivation of the overall uncertainty, justification must be provided for the assumed uncertainty distribution of that parameter.

4.2. Assurance of Quality

(51) All activities related to verification and validation of software products and input data must be carried out by suitably qualified and experienced staff who are sufficiently independent of the software developers and the persons who compiled the input data.[3]

[3] Sufficient independence is given if the persons are not the same and the V&V process is managed independently and is not distorted by resource or other constraints arising from

(52) The procedures that ensure the reduction of coding or input errors in the computer programme or calculation model must be clearly defined and justified. This must include the production of user-orientated documentation such as a user's manual, sample problems, verification or benchmark file and configuration control procedures.

4.2.1. Computer software quality assurance

In addition to the justification of the modelling process, there is a need to establish that the software products used correctly represent the physical model by ensuring that a systematic approach has been adopted for designing, coding, testing and documenting the software product.

(53) The software applied in all Evaluation Models must be validated and verified for a particular hardware and software configuration as well as a particular engineering application.

(54) The submission must contain Validation and Verification Reports for the particular hardware, software and operating system configuration used. These must list details of the hardware on which the software was run and version numbers for the supporting software such as compiler, linker, library routines and operating system. All calculations must record or reference such details.

(55) It must be ensured that the software is compatible with the hardware and the operating system (and version) of the computer installation on which it shall be run.

(56) The computer programming language used and its extensions must conform to the appropriate national, international or de-facto standards. Exceptions which may be made for COTS or Legacy Software must be justified. New coding added to Legacy Software must conform to the addressed standards unless it is a very limited alteration to existing routines and thereby avoids an extensive amount of recoding for cases where this would carry a greater risk of introducing errors or undesired numerical results changes.

(57) The algorithms used must maintain the required numerical precision and should preferably be free of numerical instabilities. If any known numerical instabilities are present the approach taken must be justified.

(58) User manuals must be suitable for their purpose and of an appropriate standard.

(59) Evidence that the software has been produced and maintained to the required standard for the application must be recorded to allow for potential inspection by NNR.

(60) It must be demonstrated in the submission that the sections of software used in the generation of the results have been adequately tested.

(61) The efforts to verify and validate software products must be documented adequately. Elements of a comprehensive documentation are V&V plans, interim V&V reports where appropriate, and final V&V reports. All this documentation must be made available to the NNR on a timely basis.

---

undue pressure for completion.

(62) In the case of non-trivial validation schemes a validation matrix linking the diverse calculation models and the applicable experiments must be included.

(63) Evidence must be included that adequate procedures are in place to control the production and maintenance of the software products, in particular change control and issuing of correct versions. Collectively these procedures are known as Configuration Management. Calculations performed to support the Safety Case must only use software products following such procedures.

4.2.2. Data quality assurance

(64) The procedures for the derivation of the input data for the calculations must also follow appropriate verification and validation procedures and must be auditable so as to assure their quality.

(65) Each item of data must have a clearly defined origin within the plant documentation or else its source must be identified and justified.

(66) Details and justification must be given of embedded data.

(67) Since it is often very difficult to fully check manually the integrity of input data, there must be suitable measures within the software to trap input data errors and erroneous results. A change control process must be established for the modification of input data.

(68) When analyses are performed with Evaluation Models employing individual programs consecutively or together, special care must be taken to document and ensure a correct and transparent transfer of data at the interfaces between the individual programs.

(69) Initial conditions and boundary conditions imposed on the calculation must be assessed to demonstrate their suitability and the related documentation must be made available to the NNR.

(70) If safety analyses are performed by means of software using Graphical User Interfaces (GUI), the program(s) must automatically record the program version details, all input used to control the program's operation, all data used for the calculation and a copy of significant output in log file(s) to be kept for the QA trail. The required content items for this file are analogous to those for non-GUI programs. GUI programs which cannot record these details must not be used for safety analysis.

4.2.3. User Proficiency

(71) The licensee must demonstrate the competence of the users to model adequately the plant and to analyse the results produced by the calculation method.

(72) Any initial deficiencies in software user experience level and knowledge must be addressed by suitable training and experience development and such experience or knowledge must be maintained to allow for any later required additional analysis work.

(73) The licensee's validation submission must contain sufficient information to enable

the NNR to make a judgement on the proficiency of the user.

A particularly important source of information about user proficiency comes from 'blind' or 'double-blind' calculations of test problems and whenever possible the submission should include such calculations.

Participation in international Standard Problem exercises where more than one participant use the same or a similar calculation method can provide a useful comparison with the abilities of other users to carry out similar calculations. In some areas (e.g. finite element analysis) accreditation schemes are in operation to define 'expert users'. Whenever possible the software users should qualify for such accreditation.

All the above requirements are applicable to all computer codes to be authorised by the NNR. However, it is recognised that in special cases such as new nuclear installation projects a stage licensing process could be applied and the demonstration to these requirements can be spread across licensing stages as indicated in section 5 below.

5. REQUIREMENTS FOR LICENSING STAGES

The following specific conditions apply to submissions on computer software and corresponding V&V, which are related to license applications for nuclear installations (e.g. power reactors) for particular licensing stages as they are defined in LG-1041 /2/.

In general the scope and depth of analysis will increase with each licensing stage as the required level of design detail increases. This implies in particular that system models to be applied to safety analysis during an early licensing stage usually cannot provide the level of detail and input data accuracy that is achievable at later licensing stages. The usual approach to cope with these uncertainties is to introduce additional margins or other mitigation measures. The verification and validation of system models required for the individual licensing stages will take the individual levels of detail into account and consider margins and mitigation measures. This is addressed by the use of the particular definition given for ‘System Model data Validation’.

5.1. Stage 1: Concept Safety Case

For the acceptance of the concept safety case the process has to include information focussed on the software used for demonstration of the safety case.

Reference can be made to past experience if justification of applicability can be given based on the criteria below.

For all calculations included in the concept safety case, the following activities must have been performed:

(74) The governing phenomena must have been identified and documented as discussed in Section 4.1.1.

(75) Appropriate mathematical formulations must have been selected.

(76) Selection (and potentially classification) of appropriate software must have been performed.

(77) If the phenomena constituting a physical process have been analysed separately then the separation of phenomena must be justified, the interfaces must be discussed, and increased safety margins must be applied which have to be documented and justified.

(78) The following steps of software V&V must be performed:

- Clarification of the V&V status
- Production of a V&V plan (including a validation matrix for non-trivial validation schemes)
- The V&V plan must have been executed at least to the following degree:
  - a Software Documentation must exist in at least a basic form.
  - the software must be verified at least in those aspects used in the Safety Case calculations.
  - the status of existing validation calculations (e.g. of HTR-applications in the past) must be clarified. At least basic validation efforts must exist or must be performed. If the existing validation calculations have to be judged insufficient regarding scope, accuracy and coverage, then higher safety margins have be introduced into the calculations. The extent of any such margins or biases must be described and justified.

(79) V&V of used system models must have been performed.

(80) V&V of the output processing must have been performed:

- Basic output written by software must be verified as representing the correct quantity with correct units.
- Post-processing software applied to software results and related input and output must be verified to ensure correct operation of all interfaces.

(81) In case of insufficient validation status of the software higher safety margins must be introduced. These higher margins must be fully documented and justified.

(82) Documentation must be issued for all of the activities associated with the above requirements and be available to NNR.

(83) Qualification of the software users must have been performed.

(84) For ‘non trivial’ software models and where only a subset of the models are being verified, validated, and used, details of how it is ensured that other models do not affect any safety analysis results must be presented.

5.2. Stage 2: Construction and Installation

In order to allow issue of a stage 2 license the following requirements must be met:

(85) The requirements for Stage 1 must have been met.

(86) All software products to be applied in the safety analysis process must have been determined.

(87) The identification of governing phenomena must have been finalised and reviewed.

(88) The selection of appropriate mathematical formulations and selection of appropriate programs must have been completed for all software to be used for safety analysis calculations.

(89) Satisfactory V&V must be presented for all software to be used for safety analysis calculations.

(90) Where a V&V plan was not executed completely, for example because required validation experiments could not be performed in time, the particular V&V status must have been assessed and correspondingly increased safety margins must have been introduced into the safety analysis calculations. Such extra margins must be fully documented and the chosen levels justified.

(91) Where the extent of the V&V completed is less than that planned the safety case submission must clarify the following factors:

- The missing V&V evidence.
- The reasons why the evidence is missing.
- The expected timescale for this evidence to become available.
- The expected evidence that will be obtained from the additional V&V when it is completed.
- The impact on the Safety Case of this missing evidence
- Clarification of the alterations made to the Safety Case to handle the absence of this additional V&V evidence
- Clarification and justification for additional margins or other measures made to satisfy the safety criteria for the current Safety Case

(92) In all cases the Safety Case presented must be self-consistent so that the V&V evidence presented is sufficient to underwrite all of the modes of plant operation considered.

(93) The following activities must have been extended to all safety analysis calculations:

- V&V of used system models must have been performed.
- V&V of output processing must have been performed:
  - Basic output written by software must be verified as representing the correct quantity with correct units.
  - Post-processing software applied to software results and related input and output must be verified to ensure correct operation of all interfaces.

(94) Related documentation for all of the above requirements must have been issued.

(95) Qualification of software users must have been performed. All users must have adequate levels of experience or training to enable the analysis to be performed to a satisfactory standard.

5.3. Stage 3: Fuel on Site, Fuel Loading, Testing and Commissioning

In order to allow issue of a stage 3 license the following requirements must be met:

(96) The requirements for the stage 2 license must have been met.

(97) The validation efforts must have been completed and Final V&V Reports must have been issued for all software used for safety analysis calculations.

However, additional subsequent system data validation efforts are allowed if it is wished to reduce or remove certain mitigation measures included in earlier submissions. These will be reviewed on a case by case basis and should be performed to the same overall standards and requirements as earlier submission work (or any higher standards that are then in force).

(98) Any new calculations performed after a stage 2 license to provide new validation evidence must have been submitted to the same V&V efforts regarding all aspects of the relevant Evaluation Models (including software V&V) and user qualification as discussed for stages 1 and 2 licensing.

5.4. Stage 4: Plant Operation

It is expected that all aspects of Evaluation Model V&V will have been completed at earlier licensing stages.

However where V&V programmes were not fully completed in the earlier Stages and extra safety margins were introduced for the Safety Case to address the deficiency further V&V evidence may now be available either from extra experimental test facilities or from plant commissioning data in particular.

Consideration will be given to proposals in the Stage 4 SAR to reduce or eliminate the extra margins introduced earlier based on new validation evidence.

(99) New V&V evidence must meets equivalent V&V content requirements to those applied in the earlier licensing Stages.

6. REFERENCES

/1/ Guidance for Licensing Submissions Involving Computer Software and Evaluation Models for Safety Calculations for Power Reactors
National Nuclear Regulator, Licensing Guide LG-1045 Rev. 0

/2/ Licensing Guide on Safety Assessments of Nuclear Power Reactor Sites
National Nuclear Regulator, Licensing Guide LG-1041 Rev. 0