Safety Guidance

Principles and Essential Conditions for the Use of Models and Computer Calculation Codes in Safety Evaluations

July 2017

BEL V

filiaal van het FANC | filiale de l'AFCN

Abstract

This document describes the basic principles of a technical procedure recommended by Bel V to ensure the validity of models and calculation results used in safety analyses, and to document the verification and validation activities.

Applicability: NA

Keywords: safety assessment - models – calculation methods – codes - verification – validation – software - computer

Classification: Public

Distribution: Unrestricted

Valid until: NA

Disclaimer Notice

This document is not intended to substitute Belgian legislative or regulatory documents, existing or future, that would by their publication overrule or replace dispositions in this document.

Bel V is not responsible, directly or indirectly, for the use by third parties of the information, guidances, processes or equipments described in this document, nor for the consequences of that use.

Table of Contents

1 Objectives and Scope

1.1 Objectives

This document describes the basic principles of a technical procedure recommended by Bel V (i) to ensure the validity of models and calculation results used in safety analyses, and (ii) to document the related verification and validation activities[1].

The objective of the approach is to obtain convincing results in these analyses. The system properties that are the objects of these analyses are of different kinds and require different types of models and calculations: *e.g.* in reactor physics (core neutronics, cooling fluid thermo-hydraulics, fuel thermo-mechanics); in evaluations of criticality, of risks of severe accidents, flows or transport for wastes.

1.2 Scope

The guidance addresses the *use* of models, calculation codes or tools in safety analyses.

It is intended for experts familiar with computer modelling and calculations tools. For calculations relevant to nuclear safety, it is assumed that the competence of the experts involved has been certified, authorised or at least confirmed.

2 Introduction and Rationale

To be convincing and acceptable beyond reasonable doubt, the justification of the properties to be demonstrated must be as ordinate and rigorous as possible. To serve that purpose, the justification process is decomposed into a sequence of logical steps. Each step is intended to produce one of the different *types* of *evidence* that are necessary and sufficient for the demonstration. These steps – called *phases* – and the *type* of the corresponding expected evidence are described in some detail in Section 4. The specific data and the amount of evidence required at each phase are application-dependent. They must be determined on a case by case basis, depending on the safety properties to be justified, and as deemed appropriate for the importance to safety of these properties. Evidence can remain valid, of course, from one case to another when models or tools are adequately re-used.

Like any creative process, this justification construction can be iterative; cycling between phases is not *a priori* excluded. Phases more likely to require backtracking to previous phases are indicated as potential halting points in Section 4.

An essential characteristic of the approach is to be driven by the properties to be demonstrated, with the aim of building an adequate *safety case*. It is thus goal-based rather than rule-based. Because it is focused on specific properties to justify, the required evidence is limited to what is necessary and sufficient for the demonstration. In this sense, it is thus more efficient for the licensee and the regulator than an approach based on rules or general prerequisites, or on a generic standard.

A real system can be apprehended by means of a *model* only. Any validation of the calculations is therefore necessarily limited to the scope and the validity of the model. This limitation is the very reason for having a model rigorously defined and validated from the outset, as complete and as coherent as possible through all phases of the multi-step demonstration.

[1] These activities are basically those specified by the Requirement *18* on the Use of computer codes within the IAEA Safety Standard "*General Safety Requirement",* No GSR Part 4 (2009): "*Any calculation methods and computer codes used in the safety analysis have to undergo verification and validation to a sufficient degree.".* One of the objectives of the assessment proposed by this guidance is to help delineate more precisely the limits of this "sufficient degree".

The guidance is formulated in terms of a limited number of basic concepts, the definitions of which conform to those of the relevant disciplines, i.e. model theory, mathematical logic and software engineering. These concepts are defined in Section 3. Terms intending to refer to these definitions appear in italics in the text. The approach takes into account – and is compatible with – the existing standards and guides in the field referenced in Section 6. A flow diagram showing the different phases of the multistep demonstration, with their inter-relations and input/output deliverables is given in Figure 1, page 17 and a nomenclature of the deliverables on page 18.

3 Basic Concepts

3.1 The Real System and its Environment

The ultimate object of the analysis is the real system (e.g. a fuel rod, a reactor coolant pressure vessel, a waste disposal…) and its interface with its natural environment. Some of the *properties* - essentially related to *safety* – have to be *justified*. The *justification* implies that these properties have to be *elicited*, *specified and evaluated*. These operations correspond to different steps of the safety justification case.

The real world can be apprehended and interpreted through *models* only. Models are described by means of *languages*, natural or formal like those of mathematics and computer programming. It is essential that models and their languages are rigorously and univocally defined, and understood by all parties involved.

3.2 The Model

More precisely, the model is a *description*, in one or more *languages*, of the real system, of its structures and its *interface* with its environment. The description must be apt at *specifying* and *evaluating* the *properties* that have been *elicited* and have to be *justified (*for instance, the limits of a radiological impact on the environment)

Typically, this description must at least include:

- The postulates and the (simplifying) *hypotheses* made on the system and its *interface*;
- The *boundaries* of the system, i.e. its interface with the environment, the system dimensions, the definition of its *state* space;
- The definition of *constants, parameters and variables*, together with their *ranges* of values;
- The *relations* between constants, parameters and variables;
- The *initial conditions* and the *boundary conditions*.

Notes:

1. *Relations* - of which equations are a special instance – are a universal modelling tool. All structures, concepts and properties, formal or not, numerical or not, can be modelled by functional, logic or mathematical relations (*cfr.* for example, §4.3 below). There is no need, therefore, to distinguish between different models: conceptual, calculation, mathematical or other. A unique, coherent and complete model of the real system and its interface should exist and contain all *relations* necessary for the *specification* and the *evaluation* of the safety *properties*.
2. The *model* is, by definition, part of the semantic basis - i.e. gives significance to the elements of the language(s) used to describe the system and to *specify* the *safety properties*. It is the unique interpretation of the real system which allows all stakeholders to understand each other. It is also used to evaluate (calculate) those properties that are quantifiable, and eventually, in some cases, to specify *validation* tests.

3. In practice, of course, the construction of the model can be gradual. It can exist in progressively more refined forms in the course of the *elicitation* (identification and elaboration), analysis and evaluation of the properties that have to be justified. But the model must remain coherent in the sense that its refined versions (*expansions*, see § 3.6 below) must preserve the semantics in order to guarantee the traceability of the safety properties through all phases of the demonstration and validation.
4. The model construction may also be the result of an iterative optimising process. Differences observed between calculation results produced by the model and measurements on the real system may be minimized by adjustments of parameter values, or by refinements of relations or hypothesises.

3.3 Description Tool(s) and Languages

Different means of *description* may be needed to describe the constituents of the *model*: natural language (or a well-defined subset thereof), mathematical equations, tabulations, graphical notations or others.

Note: Obviously, the syntax and semantics of these means of description must be apt to represent the necessary concepts, structures and behaviours, and must be defined rigorously so as to avoid ambiguities.

Example: **Phase 2** (§4.2) is the elaboration of the description of the model of the system and of its interface to its environment.

3.4 Safety Properties and Elicitation

By *safety properties* we mean the properties[2] of the real system that are the object of the analysis and have to be justified. These properties define, for instance, requirements on the performances of the real system, on its radiological impact, on the accuracy of the analysis, the time scales to be considered, etc.

Elicitation process: The elicitation of a property is the recognition and the identification of the property, and the elaboration of a first initial formulation - possibly in natural language.

Example: **Phase 1 (**§4.1) is the phase of *elicitation* of the safety properties and criteria that have to be justified.

3.5 Specification

In this document, a « *specification* » is to be understood as the precise formulation of a *property* or a *requirement* in terms of *relations* between the elements of a predefined *model*.

Example: **Phases 3** (§4.3) and **5** (§4.5.1) respectively produce the specifications of the safety properties and of the requirements for their evaluation.

3.6 Specification Translation Process and Model Expansion

A set of specifications formulated on a given model, can be translated into another set formulated on a more refined version (*expansion*) of the model. Intuitively, a *model* is an *expansion* of another *model* if it has the same sets of parameters, variables, constants and relations, possibly augmented by additional sets.

Example: **Phase 5** (§ 4.5.1) carries out the translation between two sets of specifications: from the safety property specifications into their evaluation requirement specifications.

[2] Although less general and not covering all possible cases, the term « function » sometimes is used.

3.7 Validation

In this document, *validation* is distinguished from *verification* (*Cfr*. §3.8) and is used in the classic sense. *Validation* is meant as an interpersonal recognition by consensus that a (set of) assertion(s) is objectively true and founded on a justification by *elements of proof (evidence)*, possibly diverse but in agreement. More specifically, *validation* is used in this document in three contexts:

- The *validation* of a *model* means the provision of the evidence which justifies that the *model* is *valid*, i.e. is a correct, complete and consistent representation of the *real system* and its environment.
- The *validation* of a *specification* means the provision of evidence which justifies that the formulation of the *specification* is *valid*, i.e. correct, complete and consistent in reference to the *real system* and its environment.
- The final validation of the *safety properties* means the provision of evidence which justifies that these properties are satisfied by the *real system.*

Example: **Phases 4** is the *validation* of the *model* (§4.4.1) and of the *specifications* of the *safety properties* (§4.4.2) and of *the real system* (4.6). **Phase 5** is the *validation* of the final results of the safety *evaluation*.

3.8 Verification

In this document, *verification* designates a control operation (a comparison) of the output (most often a document of *specifications* or data) produced by one phase of the demonstration with respect to the product of a previous phase (most often a document of *specifications*) – in order to establish conformity between both.

Example: **Phase 6** is the *verification* of the evaluation requirement *specifications* against the safety property *specifications* (§4.5.2), and **Phase 7** (§4.5.3) the *verification* of the results of the calculations against the evaluation requirement *specifications.*

3.9 Evaluation

Evaluation is a process of calculation or simulation which produces the result data which allow values TRUE or FALSE, to be assigned to the relations of the *model*, which are the *specifications* of the safety properties to be justified.

Example: **Phase 8** (§4.5.4) is a phase of *evaluation.*

4 Process and Method of Verification and Validation

4.1 Phase 1: Elicitation of the safety properties

The first step is the *elicitation* of the *safety properties* (see §3.4) that will have to be specified / evaluated / justified.

Notes:

1. *Elicitation of the safety properties* usually is the objective and the result of a previous *safety assessment* of the real system and its environment. This assessment is conducted by experts who have the knowledge of the real system and its environment, and of its expected behaviour taking into account the perturbations and possible hazards that can be anticipated.
2. This *elicitation* identifies the objectives of the justification: the ‘what’ and not the ‘how’. Therefore, it is important that it remain independent of the methods and tools that will be used for

the *evaluation*. Simplifications, compromises or approximations that may be required by calculation methods and tools have to be explicitly documented and accepted in **Phase 6** (deliverable **D6.2**), and not here; it is important, for traceability, to keep them separate from the safety objectives of the justification.

Input to Phase 1:

Available references to possibly existing documents on which experts base the *elicitation*.

Deliverable of Phase 1:

D1: *Elicitation* by experts of the *safety properties* that must be justified.

4.2 Phase 2: Description of the model of the real system and its interface with the environment

The physical and the time behaviour of the system and of its interface must be described by a model, the constituents and the relations of which are necessary and sufficient for the *specification* of the safety properties. Typically:

- The *boundaries* of the system (interface with the environment and other systems, inputs and outputs);
- The geometry and dimensions in space ;
- The set of system and environment *states*;
- The time scales and/or phases of interest;
- The definition of constants, parameters and variables;
- The ranges of value of constants, parameters and variables, including, when applicable, measurement units, precision levels, uncertainties on measurements and possible variations between real and represented values;
- The physical and time *relations* between constants, parameters and variables;
- The initial condition relations ;
- The postulates and simplifying assumptions made about the system and its environment ;
- etc.

Input to Phase 2:

D1.

Deliverable of Phase 2:

D2.1: *Description* of all the elements of the *model,* of the *relations* between these elements, of the set of *states*, of the *assumptions*.

D2.2: The limits of applicability of the model. The model might have been defined to cover a specific set of phenomena, of steady-state or transient processes, of environmental conditions outside which it is not pertinent.

Note: As already said in ***Note* 2** of § 4.1, the simplifying assumptions in **D2.1** must not anticipate, include or be confused with the simplifications, compromises or approximations that may result from the limitations of calculation methods or tools.

4.3 Phase 3: Specifications of the safety properties

At this stage, the *safety properties* elicited in phase 1 must be rigorously *specified* within the model of the real system and of its environment. These *specifications* are nothing else but *relations* between elements of the model[3].

As said in ***Note 1*** of §3.2, the universal character of relations allows the specifications of system functional properties (functions, equations) as well as non-functional properties (reliability, availability, accuracy, etc.); the latter being defined, for instance, in terms of probabilities, inequalities , logic relations, relations on sets, etc.

Note: Mathematical functions and equations may, and should be used in **Phases 2** and **3** to describe the model and to specify the safety properties if they are essential and necessary to the exactness of these descriptions and specifications.
Their complexity, however, should not hinder the comprehensibility of the stakeholders who are in charge of their validation (**Phase 4** here below). Besides, these mathematical formulations should not imply by themselves additional assumptions or limitations that are not inherent to the physical and time behaviour of the system and its interface as described by the model in **Phase 2**. Nor should they impose by themselves restrictions on the possible evaluations and calculations to be carried out in **Phases 5** and later.
These cautions aim at remaining in line with the qualities required from the *model* for the interpretation of the real system (*Cfr*. **Note 2** in § 3.2), for the *elicitation* of the safety properties (*Cfr*. **Note 2** in § 4.1) and their comprehensibility by all stakeholders (See **Note 2** in Section 4.4 here below). In those cases where these cautions could not be satisfied, these mathematical formulations should be integrated into the evaluation specifications defined in § 4.5.1 (**Phase 5**). and verified in **Phase 6**.

Input to Phase 3:

D1, D2.1 et **D2.2**.

Deliverable of Phase 3:

D3*: Specifications* of the *safety properties* in terms of *model relations*.

4.4 Phase 4: Validation of the model and of the specifications of the safety properties

4.4.1 The *model* must be *validated*. In practice, this *validation* implies the justification of the choice of the elements defined in § 4.2, in particular the acceptance of the assumptions, retained dimensions, initial and boundary conditions, time scales, limits of applicability, etc.
More precisely, the *model* must be shown to be:

- *Correct* : every relation expected to be evaluated to the value *true* within the model must be shown to be true within the real system and its environment ;
- *Consistent* : from the model assumptions and postulates, no relation can be derived such that this relation and its negation are true ;
- *Complete*:
    - all variables, constants, parameters and relations (deliverable **D2.1**) necessary for the *specifications* of the safety properties and their *final validation* (§4.6) are part of the model, with adequate value domains. This property is important. In the last phase of *validation* (**Phase 9**), the results of the evaluation will have to be validated and confronted with the real system – essentially through tests and data from the real system . Thus, it is necessary that all the variables, constants and parameters - that

[3] The term « safety criteria » is sometimes used to refer to some of these *specifications*.

will be subject to measurements or observations in this *final validation* - are included within the model.

- The limits of applicability of the model (deliverable **D2.2**) must be judged acceptable.

4.4.2 The specifications of the safety properties, formulated in terms of model relations in deliverable D3 at phase 3 must also be validated with respect to the safety properties elicited in phase 1. Being more precisely formulated, these D3 relations are indeed a specific interpretation of the safety properties elicited in phase 1. This interpretation must be validated.

Notes

1. Obviously, credible *evidence* supporting these *validations* 4.4.1- 4.4.2 can be produced by experts of the real system and its environment only. Typically, these experts can be the same as those who have proceeded to the eliciting of the safety properties (Cfr. § 4.1, ***Note*** 1).

2. The *validation* of the model and its *specifications* is a central and critical phase of the safety evaluation process. When not properly carried out, it is known to be an important potential source of misunderstandings and misinterpretations of the calculation results and their applicability. The experts must ensure that the model *description* and the *specifications* are accurate, unambiguous and comprehensible by all stakeholders. Nothing, and in particular no language (natural or formal), nor any mode of expression (mathematical, graphical) should prevent any person involved in the *validation* phase from fully exercising his or her engineering judgement, including the necessary treatment of inherent uncertainties, required to complete the task and achieve a consensus.

Input to Phase 4:

D1, D2.1, D2.2 and **D3**.

Deliverables of phase 4:

Two deliverables from the experts:

D4.1:

- Giving arguments and evidence of the *validity* of the *model* (completeness, consistency, correctness), as it is described in deliverable **D2.1**;
- *Validation* of the limits of applicability of the *model* defined in deliverable **D2.2**;
- Identification of deficiencies in the *model*, possibly detected by the experts, and specification of corresponding corrective actions. **Phase 4** and the following phases should not be concluded before a **final version of D4.1** confirms that these corrective actions have been taken into account.

D4.2:

- Giving arguments and evidence of the *validity* of the *specifications* of the *safety properties* (Deliverable **D3**) with respect to the *safety properties elicited* in **D1**;
- Identification of deficiencies in the *specifications* possibly detected by the experts, and specification of corresponding corrective actions; **Phase 4** and the following phases cannot be concluded before a **final version of D4.2** confirms that these actions have been taken into account.

D4.3:

- *Specification* of tests and measurements campaigns that have to be planned for the *final validation* of **phase 9**.

4.5 Evaluation of safety properties

At this stage, the *specifications of the safety properties*, validated together with their model in **phase 4**, must now be *evaluated*. This *evaluation* is at the heart of the justification process.

More precisely, all the *relations* of **D3** (Cfr. § 4.3) that describe *specifications* must be *evaluated* and shown to take the logical value TRUE within the *validated model* (Cfr. § 4.4).

This *evaluation* is the work to be achieved by tools/codes of computing, simulation and/or tests. It consists of three *specification* and *verification* steps, i.e. those **of phases 5, 6** and **7** here below.

4.5.1 Phase 5: *Evaluation Specifications* for the calculation tools (programs/ computing codes/ simulators)

The *specifications* of the *safety properties* of deliverable **D3** (§ 4.3) must be translated into *specifications* of *evaluation requirements* (hardware/software) for the calculation tools/codes, taking into account the limits of applicability and the corrective actions of deliverables **D2.2 and D4.2**

These *requirement evaluation specifications* are of two types: functional (specifying the functions to be calculated, the equations, the methods of calculation, the initial and boundary conditions …) and non-functional (specifying accuracy, mesh, convergence, response time, calculation time, man-machine interface…).

Note: The *requirement evaluation specifications* are primarily dictated by these functional and non-functional calculation needs and somewhat tool-independent in the sense that, in some cases, they may not entirely fit with the functionalities and qualities provided by - and implemented in the available calculation tools/codes that are retained. See § A.1.1.14.5.2.3.

Input to Phase 5:

D3, D2.2.

Deliverables of Phase 5:

D5.1: Functional *Evaluation Specifications* for the calculation tools (programs, calculation codes, simulators, etc.).

D5.2: Non-functional *Evaluation Specifications* for the calculation tools.

D5.3: The limits of applicability of the calculation methods being used, the approximations and the necessary empirical correlations and extrapolations.

4.5.2 Phase 6: Verification of the Evaluation Specifications

4.5.2.1. *The* functional and non-functional *evaluation specifications* of deliverables **D5.1**, **D5.2** must be *verified* against the *safety properties specifications* defined in **D3** and validated in **D4.2**; that is, the *relations* of every specification in **D3** must be shown satisfied by the *relations* **D5.1, D5.2**.

⇒ *Example:* This verification may address the conformity of the *relations* **D3** with a system of partial differential equations, or with a mesh for finite element method.

4.5.2.2. *The limits of applicability of the calculation methods, of the approximations, correlations, possible extrapolations specified in D5.3 must be shown to conform with the specifications D3 and with the limits of applicability of the model specified in D2.2.*

4.5.2.3. *If the evaluation specifications established in Phase 5 are not met by the calculation tools/codes used for the computations, the non-conformities must be reported and recommendations for corrective actions must be proposed.*

***Note*:** Some *evaluation specifications* can be verified by using analytical solutions justified relevant.

Input to Phase 6:

D2.2, D3, D5.1, D5.2 and **D5.3.**

Deliverable of phase 6:

D6.1: Verification Report of the functional and non-functional evaluation specifications.

D6.2:

- Report on the conformity of the calculation methods, approximations, correlations and extrapolations with the *evaluation specifications*;
- Identification of possible non-conformities and recommendations for corrective actions. **Phase 6** and the following phases cannot be closed before a **final version** of **D6.2** confirms the completion of these corrective actions.

4.5.3 Phase 7: *Verification* of the implementation of the *evaluation specifications*, and of the calculations

Two types of implementation must be distinguished:

a. If new software needs to be developed (programmed) or new equipment needs to be used, the different implementation phases of these new developments must be verified against the *evaluation specifications* **D5.1, D5.2, D5.3**, by following the standards and good practice guides applicable in the domain, and if necessary by taking into account the safety class of the *real system* (for ex. IEC 60880, IEC 61508, or the IEEE standards).

b. If existing tools, calculation codes or simulators are used, their correct operation, and the conformity of their performances with the non-functional *evaluation specifications* **D5.2** (numerical accuracy, etc.) and the limits of applicability **D5.3** must be justified.

Note: These verification tasks can be credited with evidence from operation feedback and/or software or equipment independent certifications (in particular for operating systems, compilers and programming or computing tools).

Input to Phase 7:

D5.1, D5.2, **D5.3** and **applicable development and implementation standards**.

Deliverable of Phase 7:

D7:

- Identification of applicable development standards, and Report of the Verifications and Validations of the implementation required by these applicable standards;
- Justification of the compliance with installation/platform dependent directives imposed by the tools being used;
- Identification of possible non-conformities and recommendations for corrective actions. **Phase 9** cannot be closed before a **final version** of **D7** confirms the completion of these corrective actions.

4.5.4 Phase 8: Evaluation

Execution of the calculations/simulations.

Note: This execution amounts to assigning a value "TRUE" or "FALSE" to the functional *relations* **D5.1** of the *Evaluation Specifications of* **Phase 5**. It is the purpose of the *verifications* carried out in **Phases 6** and **7** to ensure that these results conform with the **D3** *specifications* of the safety properties which, together with the *model*, have been *validated* in **Phase 4**.

Input to Phase 8:

D5.1, D5.2, **D5.3**

Deliverable of phase 8:

D8: Result data of the calculations/simulations; log files, warnings, notable events, execution times.

4.6 Phase 9: Final Validation

Finally, it is standard engineering practice, to cross-check, **whenever possible**, the whole verification and validation process carried out in **Phases 1** to **8**, by comparison with measurements on the *real system*. The results obtained in **Phase 8** by the calculations / simulations must be compared with measurements obtained from *the real system*, for example by reproducing measurement data obtained in situ on *the real system* in its *environment* or, when this is not feasible, by reproducing experimental data obtained from other real systems and environments judged equivalent or representative[4].

Besides:

- The results and conclusions of comparative analyses (benchmarks) by means of model variants should be evaluated and validated;
- Tests of "separate effects" and "integrated effects" should be specified and executed, and their respective coverages justified;
- Tests should control the sensitivity of conservatisms and/or of "best estimates" calculations, and justify their validity. If required, the predictive properties of the *model* and of the calculation method must be compared with other models/methods.

[4] This equivalence between two systems with their respective interfaces requires that the two models satisfy certain properties, in particular consistency between appropriate corresponding (sub) sets of their relations.

Notes:

1. In so far as the *real system* is apprehended through its *model* only, this *final validation* is also somehow necessarily piloted and directed by the *model*. This limitation is the very reason for the need from the outset of a well-defined and *validated model* (§4.2 and §4.4), which as much as possible remains complete and consistent through all steps of the demonstration.
2. This final phase may reveal discrepancies between calculation results produced by the model and measurements on the real system. These differences may require adjustment of parameter values. If these adjustments are in the scope of the parameters and do not invalidate hypotheses or other relations of the model, the model can be refined – as anticipated in note 4 of §3.2 – by iterations of phases 8 and 9.
3. This final phase may invalidate the model (e.g. its hypothesises or other relations), in whole or in part and, in this case, imply a return to **Phase 1**.
4. The final validation is a set of tests confirming that the safety properties and criteria – as they are specified in **Phase 3** and evaluated in **Phases 5, 6 and 7** – are satisfied by the real system in real conditions of operation. Often, some of these tests are not feasible before the completion of the system design. Then, a current version of the validation report (deliverable **D9**) must document this situation so as to allow an assessment of the level of validity currently achieved for the calculation results, making clear that the tests are due and postponed to the completion of the design.

Input to Phase 9:

Deliverables **D1, D2.1, D2.2, D3**, **D4.3, D8**

Deliverable of Phase 9:

D9: Final Validation Report, containing:

- The *specifications* of the tests and activities mentioned here above, the justifications of their coverages, and their results;
- Identification of possible non-conformities and recommendations for corrective actions.

Phase 9 and the justification of the *safety properties* cannot be concluded before the final version of D9 confirms a satisfactory completion of these actions.

5 Closure of the Safety Case

The deliverables which contain *terminal evidence* supporting the *justification* of the safety properties are the output deliverables which are not input deliverables to subsequent phases. The set of these output deliverables altogether contains evidence that implies the upfront evidence of the non-terminal deliverables. These terminal deliverables with the evidence they must contain are the following:

D4.1: Evidence of the validity of the model.

D4.2: Evidence of the validity of the specifications of the safety properties.

D6.1: Evidence of the conformity of the functional and non-functional evaluation specifications with the safety property specifications.

D6.2: Evidence of the conformity of the calculation methods with the evaluation specifications.

D7: Evidence of the conformity of the implementation of the calculations with applicable standards.

D9: Final Validation Report.

6 References

Standards and Guidance

[1] US NRC Regulatory Guide DG 1130 (rev. of Guide 1.152). Criteria for Use of Computer in Safety Systems of Nuclear Power Plants, 2004.

[2] US NRC Regulatory Guide 1.203. Transient and Accident Analysis Methods, 2005.

[3] US NRC Final Technical Position on Documentation of Computer Codes for High-Level, Waste Management NUREG 0856. 1983.

[4] IRSN Procédure Générale de Vérification et de Validation de Logiciels Scientifiques. IRSN / PRO-043. 2011.

[5] IRSN Scientific Computer Codes Used at the IRSN. IRSN/DSDRE/technical report n° 2010-150. 21 May 2010

[6] ASN Document sur la Qualification des Outils de Calcul Scientifique. 28/09/2011

[7] UK Nuclear Safety Directorate. Technical Assessment Guide. Containment: Validation of Computer Codes and Calculation Methods. M. Weightman. T/AST/042, issue 001. Review date 09/07/03.

[8] IEEE Standard for Software Verification and Validation Plans. ANSI/IEEE Std 10123-1986.

[9] ANSI/ANS-10.4-1987. Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry.

[10] IEEE Standard Criteria for Digital Computers in safety Systems of Nuclear Power Generating Stations. IEEE Std 7-4.3.2-2003.

[11] IEC 60880 Ed. 2 (2006-05) Logiciels pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires.

[12] Licensing of safety critical software for nuclear reactors- common position of seven European nuclear regulators and authorised technical support organisation – Revision 2015.

Related Scientific and Technical Works

[13] Les modèles mathématiques sont-ils des modèles à suivre ? Jean Mawhin, Académie Royale de Belgique, Collection l'Académie en Poche, Bruxelles, 2017.

[14] Verification and Validation in Scientific Computing. C. J. Roy, W.L. Oberkampf. Cambridge University Press, 2010.

[15] Justifying the Dependability of Computer-based Systems. With Applications in Nuclear Engineering. P.-J. Courtois. Springer. 2008

[16] Concepts of model Verification and Validation. LA-14167-MS. Los Alamos National Laboratory. Los Alamos, October 2004.

[17] The Unreasonable Effectiveness of Mathematics in the Natural Sciences. Communications in Pure and Applied Mathematics, vol. 13, No. I. New York, John Wiley & Sons, Wiley & Sons, 1960

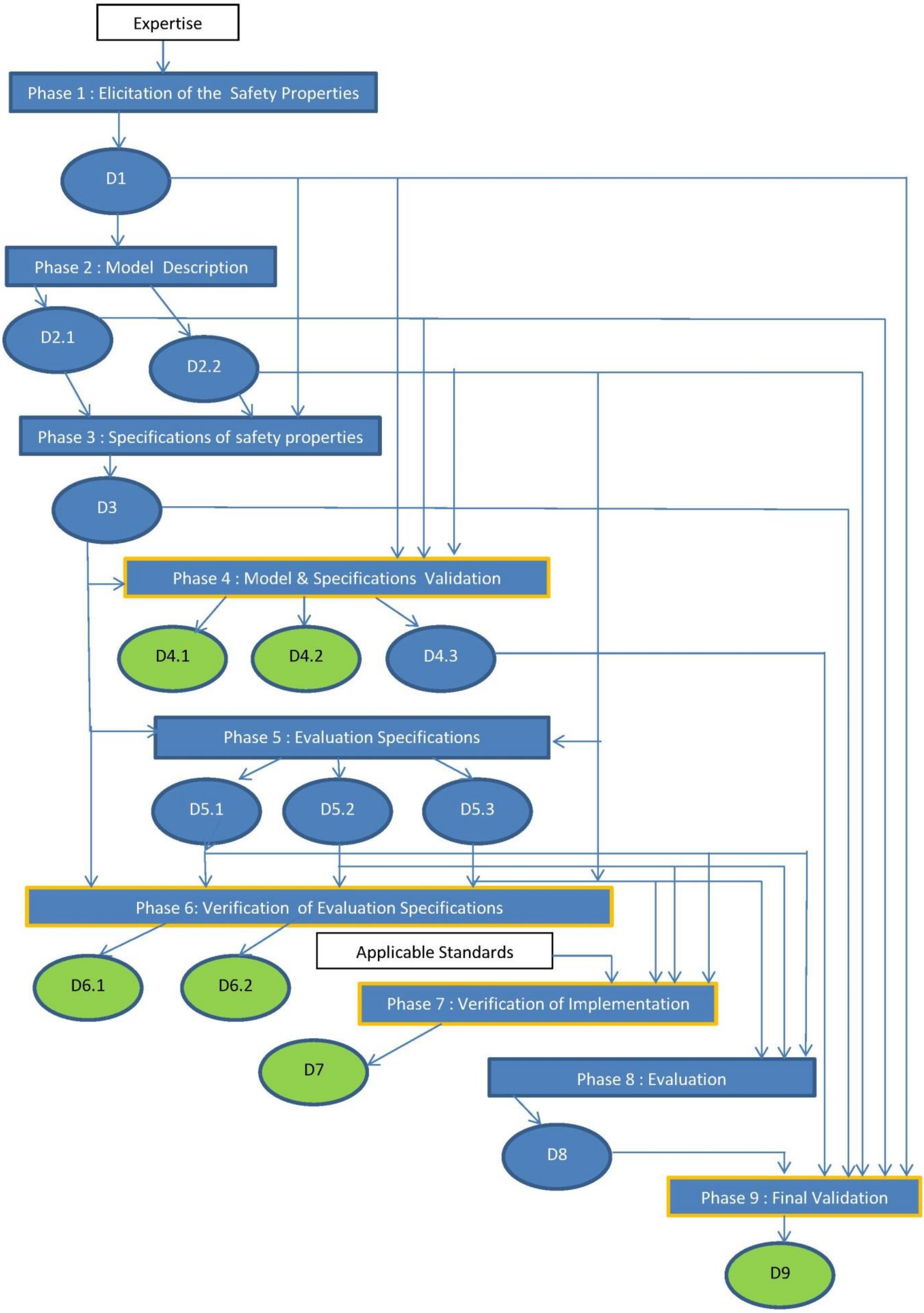
Expertise
Phase 1 : Elicitation of the Safety Properties
D1
Phase 2 : Model Description
D2.1
D2.2
Phase 3 : Specifications of safety properties
D3
Phase 4 : Model & Specifications Validation
D4.1
D4.2
D4.3
Phase 5 : Evaluation Specifications
D5.1
D5.2
D5.3
Phase 6: Verification of Evaluation Specifications
D6.1
D6.2
Applicable Standards
Phase 7 : Verification of Implementation
D7
Phase 8 : Evaluation
D8
Phase 9 : Final Validation
D9

Figure 1 : Illustrative schema of the procedure.
Oval green zones highlight deliverables with terminal evidence. Yellow frames highlight potential halting points. Arrows indicate origin and destination phases of deliverables.

List of Deliverables

Note: Yellow labels denote ‘halting point deliverables’; bold green text denotes ‘terminal deliverables’.

D1: *Elicitation* by experts of the *safety properties* that must be justified.

D2.1: *Description* of all the elements of the *model*, of the *relations* between these elements, of the *state* space, of the *assumptions*.

D2.2: The limits of applicability of the model. The model might have been defined to cover a specific set of phenomena, of steady-state or transitory processes, of environmental conditions outside which it not pertinent.

D3*:* *Specifications* of the *safety properties* in terms of *model relations*.

D4.1: **- Arguments and evidence of the *validity* of the *model* (completeness, consistency, correctness), as it is described in deliverable D2.1;**

- *Validation* of the limits of applicability of the *model* defined in deliverable D2.2;

- Identification of deficiencies in the *model*, possibly detected by the experts, and specification of corresponding corrective actions.

D4.2: **- Arguments and evidence of the *validity* of the *specifications* of the *safety properties* (Deliverable D3) with respect to the *safety properties elicited* in D1;**

- Identification of deficiencies in the *specifications*, possibly detected by the experts, and specification of corresponding corrective actions.

D4.3: *Specification* of tests and measurements campaigns that have to be planned for the *final validation* of **phase 9**.

D5.1: Functional *Evaluation Specifications* for the calculation tools (programs, calculation codes, simulators, etc.).

D5.2: Non-functional *Evaluation Specifications* for the calculation tools.

D.5.3: The limits of applicability of the calculation methods being used, the approximations and the necessary empirical correlations and extrapolations.

D6.1: **Verification Report of the functional and non-functional evaluation specifications.**

D6.2: **- Report on the conformity of the calculation methods, approximations, correlations and extrapolations with the evaluation specifications;**
- Identification of possible non-conformities and recommendations for corrective actions.

D7: **-Identification of applicable standards, and Report of the Verifications and Validations of the implementation required by these applicable standards.**

- Identification of possible non-conformities and recommendations for corrective actions.

D8: Result data of the calculations/simulations.

D9: **Final Validation Report, containing:**

- **The *specifications* of the tests and activities mentioned here above, the justifications of their coverages, and their results;**
- **Identification of possible non-conformities and recommendations for corrective actions.**