21st Annual Conference of the Canadian Nuclear Society
Toronto, Ontario, Canada / June 11-14, 2000

Safety Analysis Technology: Evolution, Revolution and the Drive to Re-Establish Margins

John C Luxat, Ph.D., P.Eng.
Manager, Nuclear Safety Technology
Ontario Power Generation, Inc.
700 University Avenue
Toronto, Ontario, M5G 1X6

INTRODUCTION

Over the past twenty-five years safety analysis has been undertaken on an on-going basis at Ontario Hydro (now Ontario Power Generation), in part to support the licensing of new stations and in part to address safety related issues that have periodically arisen. The analysis methodologies employed have been based almost entirely upon deterministic methods, similar in general nature to methods used in the rest of the Canadian industry and, indeed, the rest of the international nuclear industry. Associated with the deterministic methods is the need to make specific assumptions regarding physical models and parameters. These assumptions have been characterized by conservatism in their selection.

Significant conservatisms have typically been built into the physical models and analysis assumptions in order to accommodate either uncertainty in supporting knowledge or deficiencies in ability to model physical processes. These conservatisms, considered appropriate at the time, have been used to offset limitations in analysis technology and, as such, they have reflected the state of technology development.

There has been an evolution over the past two decades in the state of knowledge of safety related phenomena and physical processes and in the corresponding modeling capability. In this same period revolutionary changes in computing power have occurred. The central mainframe computer that at one time appeared to be evolving toward parallel processing supercomputers was supplanted by networked work-stations and personal computers, yielding greater power and functionality at the analyst's desk than was conceivable only years ago. However, analysis methodology has evolved relatively slowly in the corresponding period since it has been knowledge-bound rather than computing-bound. Point estimates of consequences of accidents have varied primarily in terms of the nature of assumptions applied in analysis. These changes have been denoted by qualifying phrases that primarily reflect the limitations of the methodologies – for example, the changes in analysis methods from "limit-consequence" to "best effort' to "limit of operating envelope".

A deleterious consequence of using deterministic analysis methodology and associated conservative assumptions is that events that are at the boundary of both the design basis as well as the risk spectrum - and sometimes beyond the design basis - have taken on their own reality. In fact, many people often perceive these analysis assumptions as representing a "more probable reality". This, in turn, has led to the perception of small safety margins in the design and has resulted in analysis that is not robust to perturbations in either the knowledge base or analysis assumptions. Neither of these two outcomes is conducive to supporting rationale decision making.

Efforts are underway at Ontario Power Generation to develop new safety analysis methodology that will support better definition of the Safe Operating Envelope (SOE) and, in so doing, will demonstrate that significant safety margins do exist. The safety analysis methodology development at OPG is more revolutionary than evolutionary in nature. It has an underlying probabilistic basis, currently referred to as "Best Estimate plus Uncertainty Analysis", but is intended to be more than just a particular implementation of such techniques. The urgent driver for this development effort is the need to re-establish safety margins in order that safe, reliable and less complex operation of nuclear units can be supported through analysis.

Given the changes that are occurring in the electricity market in Ontario and the impact this will have on the nuclear option, there is a need to focus on maintaining competitiveness in all activities – and safety analysis is not exempt. The features of the OPG methodology that are designed to specifically address these challenges, as well as the demographics of an aging safety analysis community, will be described in more detail in this paper. However, in order to understand the path to this new technology it is necessary to understand the historical context of safety analysis in OPG.

A historical perspective of the evolution of safety analysis technology at OPG is presented below. The key elements of the new safety analysis methodology are then described together with its relationship to other components of Canadian nuclear safety technology. This development is placed in context with similar work being conducted in the international Light Water Reactor (LWR) community.

HISTORICAL OVERVIEW

The evolution of safety analysis methodology has been neither smooth nor continuous. In reality the evolution has been discontinuous and can be related to specific events and issues that, at the time, imposed an immediacy and urgency on the objectives of the analysis. By and large, this evolution has been dominated by needs associated with Loss of Coolant Accidents (LOCA) – primarily the large break LOCA event and, within the context of the Siting Guide requirements (Ref. 1), LOCA events with ECIS impairments. Another characteristic of this evolution is that each of the changes in analysis methodology has subsequently been distorted by the conservatism applied to analysis assumptions to the extent that they have overwhelmed and, ultimately, negated any advances in physical modeling.

Five distinct safety analysis development phases can be identified together with the events and issuers that defined the needs of the period. These phases are:

- The ECIS Effectiveness Issue
- Limit Consequence Methodology
- Best Effort Methodology
- Limit of Operating Envelope (LOE) Methodology
- Best Estimate plus Uncertainty Analysis Methodology (the current phase)

The genesis of these phases and their inter-relationships is discussed below.

The ECIS Effectiveness Issue

The origins of this issue goes back to the initial licensing of Bruce NGS A in the early 1970's. The issue revolved around concerns that had been identified during design analysis regarding the effectiveness of the low pressure Emergency Coolant Injection System (ECIS), based upon gravity feed injection, to prevent significant fuel failures. This resulted in Ontario Hydro receiving a "show-cause" letter from the AECB in 1976 requesting reconfirmation by analysis of the effectiveness of the emergency core cooling systems for operating stations - at that time Pickering A was Ontario Hydro's only operating station.

The analysis tools of the period were relatively rudimentary and the regulator lacked confidence in the ability to demonstrate through analysis the effectiveness of this special safety system to perform its intended function. The state-of-the-art thermal hydraulic modeling of this era, represented by the homogenous equilibrium model (HEM) implemented in the SOPHT code (Ref. 2), was still being developed and reactor point kinetics was still the primary means to represent reactor kinetics.

The issues in contention related to the ability to deliver cold water into a hot steam-filled system (hot wall delay effects), the ability to rewet and cool the fuel, and the general limitations and uncertainties associated with the analysis tools of that period. Enhancement of physical models to address these issues was hampered by a lack of supporting experimental data against which to validate the models. Consequently, effort was placed on performing experiments in facilities relevant to CANDU designs. The early facilities involved included the Cold Water Injection Test (CWIT) facility built in 1974 at Westinghouse Canada's laboratory in Hamilton (now Stern Laboratories) and the scaled RD-12 thermalhydraulic loop built in 1976 at AECL's Whiteshell Laboratories in Manitoba. The CWIT facility, in particular, was used to generate experimental data to address channel refill and fuel rewetting behaviour for conditions involving cold water injection into a hot steam-filled fuel channel.

However, the accumulation of experimental data was of no significant benefit in resolving the issues because it was difficult to demonstrate the applicability and scaling of the data to reactor-specific conditions. The fact that the system thermalhydraulic codes could only represent homogenous two-phase mixtures (i.e. liquid and vapor phases well mixed and possessing equal velocities) limited their usefulness as a means to extrapolate the experimental results to reactor geometries and conditions. It was in the late 1970's that thought was given to developing a two-fluid code which later resulted in the development of the TUF code (Ref. 3) approximately five years later. This mirrored efforts underway in the United States that ultimately resulted in the LWR two-fluid codes RELAP (Ref.. 4) and TRAC (Ref. 5).

The effectiveness of ECIS remained an unresolved issue following licensing of the Bruce NGS A station. However, it took on a different direction in the early 1980's as a result of the development of "limit consequence" analysis methodology, discussed below.

Limit Consequence Methodology and its Impact

Limit consequence analysis methodology was developed over a short period of time starting in 1980 and ending in 1981 with the so-called "Green" and "Blue" book reports for Bruce A and Pickering A, respectively (Ref. 6, 7). The genesis of this methodology was a request from the AECB for a reanalysis of the consequences of a large break LOCA event in Pickering A and Bruce A.

A few years prior it had been established that for certain postulated LOCA events it was possible for channels in one core pass to experience sustained very low flow conditions. These conditions were referred to as "stagnation break" conditions because the analysis of that time exhibited what appeared to be stagnated channel flows for a specific break magnitude and location - a Reactor Inlet Header (RIH) break. More importantly, for these "stagnation break" conditions it was possible for pressure tubes to heat-up while still at pressure such that gross deformation due to thermal creep strain could occur – the so-called pressure tube "ballooning" phenomenon. This phenomenon, together with possible fuel bundle deformation at high temperatures, put into question the integrity of fuel channels. In turn, this raised questions regarding the effectiveness of ECIS since one of the fundamental nuclear safety tenets applied in demonstrating effectiveness was assurance of a coolable core geometry – which ultimately became synonymous with assuring no fuel channels failures.

Recognizing the inability to address the contentious issues with the HEM-based system thermalhydraulics code, SOPHT, and the difficulty to directly utilize available experimental data, Ontario Hydro adopted a bounding analysis methodology termed "limit-consequence" (Ref. 8). Explicit in this methodology was an attempt to circumvent the uncertainties in crediting ECIS coolant injection to re-establish adequate fuel and fuel channel cooling. Instead analysis assumptions were applied which deliberately bounded the possible consequences by imposing conditions that maximized the exothermic Zircaloy-steam oxidation reaction. Through parametric analysis it was established that arbitrary flows of the order of 25 to 100 g/s of steam, assumed to be superheated at the channel inlet, flowing through affected fuel channels maximized the consequence. The underlying premise of the limit-consequence methodology was that if the clearly extreme bounding assumptions could be demonstrated to yield acceptable consequences, then the need to address more realistic but less limiting conditions would not be required.

As a result of the assumed sustained low steam flow, widespread pressure tube deformation, either by early pressure tube ballooning in the broken pass, or delayed pressure tube sagging in the unbroken pass, was calculated. However, core coolability was assured by heat rejection to the moderator from deformed channels. Thus the concept of the moderator as the ultimate heat sink was established. The focus of analysis and supporting experimental programs now shifted to issues pertaining to fuel behaviour at high temperature (Ref. 9, 10) and fuel channel integrity (Ref. 11, 12, 13, 14). Experimental programs were established to quantify moderator subcooling required to assure fuel channel integrity (Ref. 15) and to study the role of contact conductance in controlling heat transfer rates between deformed pressure tubes and calandria (Ref. 16, 17).

However, defining the required moderator subcooling was necessary but not sufficient. The subcooling available during the LOCA event had also to be calculated in order to demonstrate assurance of fuel channel integrity. This led to the development of the MODTURC computer code (Ref. 18) that was designed to predict flow and temperature distributions in the moderator. Jointly developed by Ontario Hydro and Advanced Scientific Computing Limited of Waterloo, Ontario (now part of AEA Technologies) the development of this code progressed to the state-of-the-art computational fluid dynamics (CFD) code MODTURC_CLAS (Ref. 19), which is now the Industry Standard Toolset (IST) (Ref. 20, 21) code for three-dimensional moderator thermalhydraulic calculations.

The development of limit-consequence methodology also coincided with the establishment of three-dimensional neutron kinetics as an integral part of safety analysis. This was facilitated by

the deployment of the spatial modal kinetics code, SMOKIN (Ref. 22, 23), in the first limit consequence analyses. Originally developed as a tool for analysis of spatial control problems in design studies for Ontario Hydro's 1250 MW conceptual reactor design, SMOKIN was developed further for use in accident analyses and subsequently has served as the standard space-time kinetics calculation tool in Ontario Hydro for the past two decades.

Limit-consequence methodology became an established analysis approach for bounding the consequences of LOCA and was employed in the safety report analyses submitted for licensing of the Pickering NGS B, Bruce NGS B in the early 1908's and Darlington in the late 1980's (Figure 1). However, the methodology did not accommodate a clear distinction between a LOCA event with ECIS available and a LOCA event with impaired ECIS. By the very definition of the bounding steam flow assumptions, and the limited credit for blowdown cooling, the consequences of these events essentially appeared to be one and the same. More importantly, the arbitrariness of the assumptions and their disconnection from specific failure event scenarios led to the perception of LOCA and LOCA/LOECI having consequences that are more closely related to severe fuel damage events in other jurisdictions (i.e. they appeared *de facto* to be severe accidents). The phenomenology associated with limit-consequence methodology was that of a severe accident – widespread gross deformation of fuel channels, severely overheated fuel resulting in bundle "slumping", and large amounts of hydrogen gas being produced from the Zircaloy-steam reaction.

With time and continuing application of the methodology it came to take on its own "reality". What in other jurisdictions was beyond design basis severe accident behaviour became part of the design basis envelope in Canada and exerted a significant influence on a number of generic safety issues including ECIS effectiveness and hydrogen behaviour in containment.

Best Effort Methodology

During the licensing of Bruce B the issue of ECIS effectiveness resurfaced and initial attempts were made to resolve the issue within the limit-consequence framework. These initial studies, referred to as "Best Effort ECIS Effectiveness, Phases I and II" were focussed on demonstrating that the reliance on moderator as a heat sink was of limited duration. The approach adopted was to use experimental data, primarily from hot feeder refill tests performed in the CWIT facility at Stern Laboratories, together with lumped parameter approximation models of feeder hot wall delay behaviour. However, it was soon recognized that this approach did not directly address the issue of ECIS performance effectiveness and the regulator remained dissatisfied with what they considered to be the speculative nature of limit consequence methodology.

The Best Effort Phase III study was initiated in 1986 with the specific objective of providing, on a best effort basis, an estimate of the consequences of a LOCA with ECIS available. Darlington was selected as the target station. The approach adopted was to apply the recently developed two-fluid code, TUF, as a "best estimate" code to quantify the governing behaviour during the early stages of blowdown cooling and subsequent injection of cold ECIS water into the heat transport system. It was felt that the accumulated experimental data from the CWIT facility, from the RD-14 loop facility at AECL Whiteshell Laboratories, and more recently from the modified multiple parallel channel RD-14M facility provided a strong supporting basis for modeling the governing phenomena. Furthermore, there was a strong belief that the consequences of the postulated LOCA events were significantly less severe than those associated with limit-consequence methodology.

The first pilot application for a Darlington unit was completed in 1993 and a report was submitted to the regulator. The results of the analysis did indeed demonstrate a number of significant differences from limit-consequence methodology. These differences included:

- Blowdown cooling was effective in the short term in limiting the magnitude of fuel heatup during and immediately after the power pulse,
- Stagnation break behaviour was primarily a figment of simulating one flow pass in the core with one equivalent single channel – for the same header boundary conditions close to zero net flow in a core pass could be achieved by the sum of relatively high transient bi-directional flows in different groups of channels in a core pass. Furthermore, it was virtually impossible, given the differences in elevations and powers of the channels in a core pass, to have all channels in the pass behave in exactly the same manner.
- Low flow conditions could not be sustained for any length of time during blowdown because, ultimately, as the heat transport pump head degraded due to void developing at the pump suction the balance between the pump head and the break was broken.
- The ECIS was effective in re-establishing good fuel and fuel channel cooling and the timing of initiation of injection flow into the heat transport system was not very critical – injection just needed to occur during the blowdown period.

The application of this Best Effort analysis of blowdown cooling during LOCA became the standard approach used in updating the safety report analysis for the Bruce A&B and Pickering A&B stations as part of Ontario Hydro's generic safety report update program. However, before the results could be consolidated the "discovery" of fuel string relocation reactivity occurred and led to increasing conservative assumptions within the "limit of operating envelope" approach.

Limit of Operating Envelope (LOE) Methodology

The recognition of the reactivity effect associated with coherent and rapid relocation of all fuel bundle strings in the channels of the affected pass of a core during a LOCA has had a profound impact on safety analysis in Ontario Power Generation. For reactor designs such as at Bruce and Darlington where fuelling is against the flow (i.e. new fuel bundles are introduced at the outlet end of fuel channels) the reactivity addition is positive and occurs shortly after the break is initiated. The rapid positive reactivity insertion that occurs before shutdown is initiated augments the positive coolant void reactivity and exacerbates the magnitude of the power pulse – hence, this issue is often referred to as the "power pulse" problem. Additionally, the magnitude of reactivity insertion is dependent upon the pre-existing gap between the upstream end of the fuel string and the inlet shield plug – the gap being larger for older reactors due to uncompensated axial creep of the pressure tubes.

The reactors most affected by this reactivity effect were those at Bruce A&B and Ontario Hydro voluntarily derated all the units to 60% FP until compensating measures could be established to offset the effect of the additional positive reactivity insertion. Design change measures included reversing the direction of fuelling in the Bruce A reactors and introduction of long fuel bundles in Bruce B and Darlington reactors as a means of fuel string/shield plug gap management. A significant safety analysis effort was initiated both to support the design modifications and to establish restrictions on the operating envelope that would allow the power level of the reactors to be increased. Operating limits on allowable flux tilts were reduced significantly, as were limits on moderator and coolant isotopic purity and limits on moderator poison concentration.

The latter restrictions were aimed at compensating for the fuel string relocation reactivity by reducing the magnitude of the coolant void reactivity feedback.

However, a new challenge to fuel channel integrity was introduced with restrictions on the gap between the fuel string and the inlet shield plug. Relative thermal expansion of the overheated fuel string and pressure tube could result in a reduction of the gap and the possibility of constrained expansion if the fuel string expanded sufficiently to contact the shield plug. This resulted in an additional safety evaluation criterion; avoidance of constrained relative fuel string axial expansion, being introduced into the analysis.

The new safety concern and compensatory measures placed a focus on multiple operating parameter variations. Accommodation of these factors in the on-going re-analysis that was being performed resulted in a rapid change into methodology that provided bounding point estimates of consequences – now generally referred to as "limit of operating envelope" (LOE) methodology. While LOE concepts had been employed in the past the perception of the criticality of operating parameter assumptions had not been as great until the "power pulse" issue arose.

After a series of LOCA re-analyses, narrowly focussed on power pulse and constrained expansion issues, the power levels of the Bruce reactors were gradually increased. In 1996 approval to return to 94% FP, the desired Ontario Hydro power level, was obtained – only to be negated by discovery of an error in one of the safety analysis codes. The Bruce B reactors have been limited to 90% FP since that time.

No sooner had the Bruce reactors been returned to 90% FP, than a new challenge, generic to all CANDU reactors, developed. As a consequence of experimental measurements of simulated mid-burnup fuel in AECL's ZED-2 research reactor at Chalk River Laboratories it appeared that the allowance for under-prediction of void reactivity by the POWDWRPUFS-V lattice cell code was significantly lower than previously thought. Furthermore, it appeared that there was uncertainty in the WIMS-AECL lattice cell code, the code to which the industry is migrating.

As a result of reporting this preliminary research finding, Ontario Power Generation undertook a series of large break LOCA re-analyses for Bruce B with increasing values of the void reactivity error allowance (VREA) while experiments continued at Chalk River to better define an appropriate value for VREA. At each re-analysis a further tightening of operating limit assumptions were made to compensate for the increased VREA values. The net result has been a series of point estimates of consequences with assumptions that force the results, by very definition, to the edge of the acceptable region of the safe operating envelope – in the process leaving the perception of small safety margins.

Best Estimate plus Uncertainty Analysis Methodology

Results of LOE analysis notwithstanding, it are generally accepted that safety margins are, in reality, larger than current analysis indicates. However, the challenge is to demonstrate in an acceptable manner that these margins exist and quantify their magnitude. This situation is not unique to Ontario Power Generation, or the other Canadian utilities. Similar issues have faced the LWR designs. The US NRC provided an alternative to the 10 CFR 50 Appendix K prescriptive rules by allowing best estimate methods to be employed, but in so doing also required that there be a systematic quantification and accounting of uncertainties associated with the analysis. This resulted in development of a framework methodology termed CSAU (Code

Scaling, Applicability, and Uncertainty) (Ref. 24) and an application to a Westinghouse PWR design limiting large LOCA.

However, concerns remain regarding the practicability of the CSAU methodology for large scale accident analysis in an operating utility. For this reason Ontario Power Generation embarked on development of new safety analysis methodology aimed at incorporating the essential features of Best Estimate plus Uncertainty Analysis but modifying the elements to address analysis needs in the anticipated competitive future environment. The primary driver is the need to re-establish the safety margins that are believed to exist.

ONTARIO POWER GENERATION METHODOLOGY DEVELOPMENT

Development of a methodology to perform best estimate and uncertainty nuclear safety analysis has been underway at Ontario Power Generation Inc. for the past two years. The objectives of the analysis are multi-fold and include:

- Providing a basis for systematic quantification of safety margins within a best estimate framework with integrated accounting of uncertainties,
- Supporting the definition of Safe Operating Envelope (SOE) limits,
- Supporting operating compliance strategies associated with the SOE,
- Providing a formal basis for conducting safety analysis in an incremental fashion through direct incorporation of past analysis results, and
- Providing an ongoing learning and training component to support maintenance of safety analysis skill and competency.

A key driver for the methodology development project, and one of the major challenges faced, is the need to demonstrate safety margins on an ongoing basis in a cost-effective manner. This challenge is of importance given the inevitable aging of both operating plants and the nuclear safety analysis community and the transition to competition in the electricity marketplace.

This paper presents the methodology framework, identifies the elements that are key to ensuring viability within an operating nuclear utility, and presents results of prototype application for two accident categories in different Ontario Power Generation stations. The prototype applications considered are large break LOCA in a Bruce generating unit and a Loss of Flow accident in a Darlington generating unit.

Basis and Purpose of the Methodology

The underlying basis of the analysis methodology is that best estimate models of physical processes, best estimate or operating centre plant states, and most probable system configurations and failure events provide the most realistic representation of plant behaviour and consequences during accidents. Deviations from these best estimate conditions can and will occur, which will result in uncertainty in the outcome of the best estimate analysis. In order to quantify this uncertainty, it is necessary to identify and characterize the components contributing to uncertainty, and evaluate their impact on safety consequences. The primary purpose of the methodology is to define the ranges of governing parameters, within which safety objectives can be met to a prescribed level of confidence, through the use of an integrated probabilistic approach.

Furthermore, it is recognized that the safety analysis process has an underlying element of refinement whereby new information or revised models and uncertainty allowances are applied to evaluate their impact on calculated consequences. In the past, this has been accomplished by undertaking significant re-analysis, with no formal method for incorporating prior knowledge and experience. Therefore, another objective of the methodology is to provide a systematic, formal framework for incrementally incorporating new information and knowledge with prior information and knowledge, derived from existing analyses. This is a key feature designed to insure that safety analysis can be maintained current without requiring an ongoing extensive re-analysis effort.

ELEMENTS OF THE ANALYSIS METHODOLOGY

The elements of the safety analysis methodology are shown in Figure 2 and described below.

Technical Basis Definition

This element establishes the technical basis for a particular analysis. The main purpose of the technical basis is to systematically collect and document pertinent technical information that describes the underlying knowledge base. The safety concerns related to the accident scenarios under consideration (e.g. large LOCA, small LOCA, Loss of Flow, etc.) provides the specific focus for this element.

The technical basis includes the physical process behaviour exhibited during the progression of the accident; the physical phenomena that occur; and the modelling and physical representation of the plant. As such the technical basis serves as a repository reflecting current state-of-knowledge and, therefore, serves a role in knowledge transfer and training to new staff.

In particular, the following aspects are addressed in the technical basis:

Safety Evaluation Criteria

The criteria that are utilized to characterize the safety concerns and making judgements on the acceptability of the consequences of analyzed accident scenarios are collected and recorded, together with the underlying rationale supporting their use. These include, for example, criteria that are used to assess the effectiveness of reactor shutdown, such as trip parameter effectiveness criteria, the adequacy of fuel cooling, the assurance of fuel channel integrity, the effectiveness of heat sinks, the integrity of containment functions, and the acceptability of dose consequences. This information is included in the Technical Basis Document, the content of which is specified in an Ontario Power Generation Methodology Development Guideline.

Physical Phenomena

The physical phenomena, which influence the behaviour of the reactor system during an accident scenario, are collected and recorded. For each physical phenomenon, the following aspects need to be documented:

- A technical background summarizing the manner in which the phenomenon influences system behaviour during the accident scenario.

- A summary of the state of knowledge and uncertainties in quantifying the phenomenon. This includes, for example, physical models and empirical correlations that are used to simulate system behaviour, as well as their applicability with reference to supporting R&D results.

- A brief assessment of the potential impact of uncertainties in the phenomenon on expected behaviour during the accident.

- A list of related phenomena (i.e. other phenomena that are influenced by, or which influence the phenomenon being described).

- A list of references to papers, reports and other documents that describe or quantify the phenomenon.

This information is included in the Technical Basis Document as per specifications in an Ontario Power Generation Methodology Development Guideline (*Guideline for Preparation of Technical Basis Documents).*

Validation Matrices

CANDU validation matrices have been developed for all the major disciplines involved in accident analysis (Ref. 25). They identify and rank key physical phenomena for the accident scenario under consideration and identify the experimental database that is available for validating the relevant phenomena modelled by computer codes. The validation matrices are employed in developing the validation plans for specific computer codes and also provide systematic collations of historical R&D information.

Plant State Characterization

The technical data and information that is necessary to characterize and quantify the plant operating state and equipment and system configurations are collected and recorded. Typically, this information is derived from technical surveillance and system testing at site, and from design documentation.

Existing Analyses

Information from previous analyses, including identification of computer code versions, physical models used, assumptions and input data, and result files and documentation are assembled and referenced.

Analysis Basis Definition

This element establishes the basis for a particular analysis to be performed by systematically collecting and recording pertinent technical information relating to the computer codes to be used, their applicability to the analysis, assumption to be applied, and the reference data sets that represent the plant and physical models. In particular, the following aspects are addressed in the analysis basis:

Computer Codes and Physical Models

The versions of the computer codes to be used, together with references to the associated models that represent the underlying physical phenomena, are collected and recorded.

Computer Code Applicability

The applicability of computer codes for the safety analysis application needs to be established through relevant computer code validation. Based on the relevant validation matrices, computer code validation exercises are performed. The applicability of the computer code to the analysis is established with reference to the validation that has been performed.

Best Estimate Basis

The assumptions and supporting data that define best estimate conditions are collected and recorded. This may include assumptions relating to best estimate physical models and best estimate or "operating centre" Plant State. This information includes such items as safety evaluation criteria, physical and geometric modelling and plant characterization data.

Accident Scenario Characterization

The possible failure events and combinations of plant states that are to be considered in the analysis are identified. This establishes the analysis structure and scope. Through consideration of event combination frequencies and potential consequences, an appropriate set of safety evaluation criteria are selected which reflect approximately equal risk. Deterministic criteria (e.g. number of shutoff rods available, backup trip credited, etc.) can be applied via the assignment of appropriate probabilities such that they can be used in the integrated uncertainty analysis.

Additionally, the manner in which existing analysis results collected in the Technical Basis are to be employed, either to generate or validate Physical Interdependency Functional Relationships (see below) is specified.

Phenomena and Key Parameter Identification and Ranking

The phenomena and parameters that are of importance in postulated accidents are systematically reviewed and assessed. The outcomes of this systematic review are the Phenomena and Key Parameter Identification and Ranking Tables (PKPIRTs). The content and method of preparation of PKPIRTs is specified in an Ontario Power Generation Methodology Development Guideline (*Guideline for the Preparation of Phenomena and Key Parameter Identification and Ranking Tables*).

The parameters in a PKPIRT include the operational values of process variables, such as pressures, flows, temperatures and levels; reactor core state parameters, such as bulk and regional powers, flux tilts, and bundle and channel powers; parameters that relate to reactor safety systems, reactor and process control systems; parameters that characterize the physical geometry of equipment and components; and values of parameters used to model systems, components and physical processes in the computer analysis codes.

In the initial PKPIRT parameters are ranked according to their impact on relevant accident consequences, as quantified by the safety evaluation criteria. This focuses attention on a smaller set of key parameters that are important in an accident event. The final PKPIRT reflects the outcome of the analysis and summarizes the relative importance of the key parameters to the various safety concerns.

Physical Interdependency Functional Relationships

Functional relationships that describe the underlying physical interdependencies between parameters are developed. These relationships, which are used as a basis for quantification of the sensitivity of plant behaviour and specific safety consequences to the identified key parameters, are called Physical Interdependency Functional Relationships (PIFRs). This is a novel feature of the Ontario Power Generation methodology and is based upon the considerable body of work in the areas of Dynamic Systems Theory, Automatic Control Theory and System Identification.

Three levels of ascending detail are specified as acceptable means to generate PIFR, ranging from non-linear polynomial function fitting commonly used in response surface generation techniques to non-linear coupled differential equation representation of dynamic sensitivity based upon the variational methods of modern control theory.

These functions provide the basis for generating Functional Response Surfaces (i.e. the variation in a dependent parameter to combinations of variations of independent key parameters) and, in turn, provide the means for quantifying the integrated uncertainty in the quantitative safety criteria. They also provide the means for evaluating the sensitivity functions that are necessary for quantification in the PKPIRT process.

The requirements related to PIFRs, and their application to generate Functional Response Surfaces, are specified in an Ontario Power Generation Methodology Development Guideline (*Guideline for the Preparation of Physical Interdependency Functional Relationships and Functional Response Surfaces*).

Quantification of Uncertainty Components

All sources of uncertainty that influence the key parameters in an analysis, and hence contribute to the uncertainty in quantifying a safety concern, are systematically identified, classified, and quantified.

Identification and classification is the process of determining the nature of the uncertainty, that is, whether it is a systematic bias or whether it represents a random variation around a best estimate value. Quantification is the process of determining the values for a statistical model that describes the expected variability of parameters.

The sources of uncertainty to be quantified include:

- uncertainties related to the state of knowledge of physical processes and phenomena (typically from interpreting R&D results),

- uncertainties related to plant state, including plant process parameter variation,

- uncertainties related to plant system functional performance variation (e.g. setpoints, instrumentation delays, system response versus time), and

- uncertainties related to modeling physical behaviour (e.g. computer code uncertainty)

The process to be used in specifying best estimate parameter values and parameter uncertainty is contained in an Ontario Power Generation Methodology Development Guideline (*Guideline for Specification of Best Estimate and Uncertainty Values for Plant and Modeling Parameters*)

Integrated Uncertainty Analysis

The probability of acceptable safety consequences, as defined by the safety evaluation criteria, is quantified. The integrated uncertainty analysis uses the PIFR-based Functional Response Surfaces to generate outcomes that determine the conditional probability that a safety evaluation criterion will be exceeded as the underlying key parameters vary according to their defined statistical model of variability.

The results of the integrated uncertainty analysis provide the basis for quantifying safety margins to a specified level of statistical confidence. The ranges in parameter space for which safety consequences are acceptable, at the specified level of confidence, define a portion of the Safe Operating Envelope.

The process to be used in performing integrated uncertainty analysis is contained in an Ontario Power Generation Methodology Development Guideline (*Guideline for Integrated Uncertainty Analysis)*

APPLICATION OF THE METHODOLOGY

Application of the nuclear safety analysis methodology to date has been as follows.

Darlington Loss of Flow

A licensing quality submission of best estimate plus uncertainty analysis of a single heat transport pump trip in a Darlington unit was submitted in April 2000. This analysis was in support of a new ROH-to-ROH differential pressure trip designed to provide backup coverage for loss of flow events and allow the units to return to full power operation.

This analysis successfully demonstrated the effectiveness of both primary and backup trips to meet safety design criteria at high confidence levels (95%/95%) with significantly larger margins relative to LOE analysis.

Bruce B Large LOCA

A prototyping best estimate plus uncertainty analysis was submitted to the regulator as part of a commitment to develop the new safety analysis methodology. The results of this prototyping analysis were positive in that they demonstrated significant larger margins relative to LOE analysis to fuel centreline melting, fuel sheath melting and constrained fuel string axial expansion. Additionally, the preliminary results also indicated a low probability of pressure tube

ballooning during the large LOCA, which is significantly different from limit consequence and LOE results.

An important feature of the Bruce B application was that no new analysis was performed specifically to support the application of the new methodology. Existing analysis dating back to the Safety Report update in 1994 was solely employed. This demonstrated the feasibility of implementing an incremental analysis approach as opposed to one involving large-scale reanalysis.

CONCLUSIONS

The evolution of safety analysis technology over the last two decades at Ontario Power Generation has been presented. The major issues that have shaped this evolution were described. The impact of adopting the limit consequence approach in the early 1980's has been major and has tended to distort the perception of consequences of LOCA accidents toward the more improbable severe accident domain at the expense of the more realistic design basis events.

The current effort to develop a new safety analysis methodology based upon a Best Estimate plus Uncertainty Analysis framework is aimed at re-establishing safety margins that are believed to exist and are expected to be large than those associated with deterministic limit of operating envelope analysis.

Based upon experience with applying this methodology it appears that the re-establishment of demonstrated margins is achievable. However, significant work remains to gain acceptance of the methodology and, based upon the historical evidence, avoid having the methodology drift once more into the domain of bounding conservatism.

REFERENCES

1. D.G. Hurst and F.C Boyd, "Reactor Licensing and Safety Requirements", Paper 72-CNA-102, Presented at the 12th CNA Conference, Ottawa, June 1972.

2. Chang, C.Y.F. and Skears, J., "SOPHT - A Computer Model for CANDU-PHWR Heat Transport Networks and their Control", Nuclear Technology, Vol. 35, (October 1977).

3. W.S. Liu, W. Yousef, J. Pascoe, A, Tomasone, M. Williams and J.C. Luxat, "TUF: A Two-Fluid Code for Thermalhydraulic Analysis", Proc. 10th Canadian Nuclear society Conference, Ottawa, June 4-7, 1989.

4. V.H. Ransom, et.al., "RELAP5/MOD1 Code Manual, Volume 1, 2, and 3", NUREG/CR-4312, EGG-2396., August, 1985.

5. "TRAC-PF1/MOD1: An Advanced best-Estimate Computer Program for Pressurized Water Reactor Thermal-Hydraulic Analysis", NUREG/CR-3858, LA-10157-MS, 1986.

6. "Bruce NGS A - Assessment of Large Break Loss of Coolant Accident", Ontario Hydro Design and Development Division Report No. 81038, February 1981.

7. "Pickering NGS A - Assessment of Large Break Loss of Coolant Accident", Ontario Hydro Design and Development Division Report No. 81157, April 1981.

8. R.A. Brown, C. Blahnik and A.P. Muzumdar, "Degraded Cooling in CANDU Reactors", Nuclear Science and Engineering, 88(3), 1984.

9. Hadaller, G.I., et al, "Experiments Investigating the Thermal Mechanical Behaviour of CANDU Fuel Under Severely Degraded Cooling", Proceedings Fifth International ANS/ENS Thermal Reactor Safety Conf., Karlsruhe, (September 9-13, 1984).

10. Wadsworth, S., et al, "Experimental Investigation of CANDU Fuel Deformation During Severely Degraded Cooling". Proceedings International ANS/ENS Topical Meeting on Thermal Reactor Safety, San Diego, California, USA, February 2-5, 1985.

11. Muzumdar, A.P., "Generic Aspects of Fuel Channel Integrity During LOCA Scenarios", Ontario Hydro, Design and Development Division, Report No. 82028, March 1982.

12. Kundurpi, P.S. and Archinoff, G.H., "Development of Failure Maps for Integrity Assessment of Pressure Tubes", 7th Annual CNS Conference, Toronto, June 1986.

13. Archinoff, G.H. and Kundurpi, P.S., "Pressure Tube Integrity During Ballooning with a Non-Uniform Circumferential Temperature Distribution", OH-DD-84433, November 1984.

14. Archinoff, G.H., Lowe, P.D., Luxat, J.C., Locke, K.E., Muzumdar, A.P., So, C.B. and Moyer, R.G., "Simulation Methodology for Pressure Tube Integrity Analysis and Comparison with Experiments", Proc. Second International CNS/ANS Conference on Simulation Methods in Nuclear Engineering, Montreal, October 1986.

15. Gillespie, G.E., "An Experimental Investigation of Heat Transfer From a Nuclear Reactor Fuel Channel to Surrounding Water", Proc. CNS 2nd Annual Conference, June, 1981.

16. Gillespie, G.E., et al, "An Experimental Investigation of the Creep Sag of Pressure Tubes Under LOCA Conditions", CNS 5th Annual Conference, June 1984.

17. Gillespie, G.E., R.G. Moyer, and G.I. Hadaller, "An Experimental Investigation Into the Development f Pressure Tube/Calandria tube Contact and Associated Heat Transfer Under LOCA Conditions", CNS 6th Annual , Ottawa, June 1985.

18. Szymanski, J., et al., "Comparison of MODTURC Predictions with Moderator Temperature Measurements in Bruce NGS Unit 3 and Pickering NGS Unit 5", Appendix A. "MODTURC: Equations and Algorithm", Ontario Hydro, Design and Development Division, Report No. 84177,1984.

19. R.G. Huget, et.al., "MODTURC_CLAS: An Efficient Code for Analyses of Moderator Circulation in CANDU Reactors", Proceedings 3rd International Conference on Simulation Methods in Nuclear Engineering, Montreal, April, 1990.

20. J.C. Luxat, V. Snell, M.-A. Petrilli, and P.D. Thompson, “The Industry Standard Toolset Initiative”, Proceedings CNS Annual Conference, Montreal, June, 1999..

21. J.C. Luxat, W. Kupferschmidt, P.D. Thompson, and M.-A. Petrilli, “The Industry Standard Toolset (IST) of Codes for CANDU Safety Analysis”, to be presented at OECD/CSNI Workshop on Advanced Thermal-Hydraulics and Neutronic Codes: Current and Future Applications, Barcelona, Spain, April 10-13, 2000.

22. Luxat, J.C. "The Potential of a Generalized Modal Analysis Method in the Design and Analysis of CANDU--PHW Reactor Control and Safety Systems," 18th Annual Int. Conf. Canadian Nuclear Association, Ottawa, June 1978.

23. Luxat, J.C., and Frescura, G.M., "Space-Time Neutronic Analysis of Postulated Loss-of-Coolant Accidents in CANDU Reactors", Nuclear Technology, Vol. 46, 507-516, December 1979.

24. Quantifying Safety Margins: Application of Code Scaling, Applicability, and Uncertainty Evaluation Methodology to a Large Break Loss-of-Coolant Accident, NUREG/CR-5249, EGG-2659, 1989 – also Nuclear Engineering and Design, 119, 1990.

25. E.O. Moeck, J.C. Luxat, L.A. Simpson, M-A. Petrilli and P.D. Thompson, “ Validation of Computer Codes used in Safety Analysis of CANDU Power Plants”, Proc. IAEA Technical Committee Meeting on Advances in Heavy Water Reactors, Bombay, India, Jan 29-Feb.1 1996.

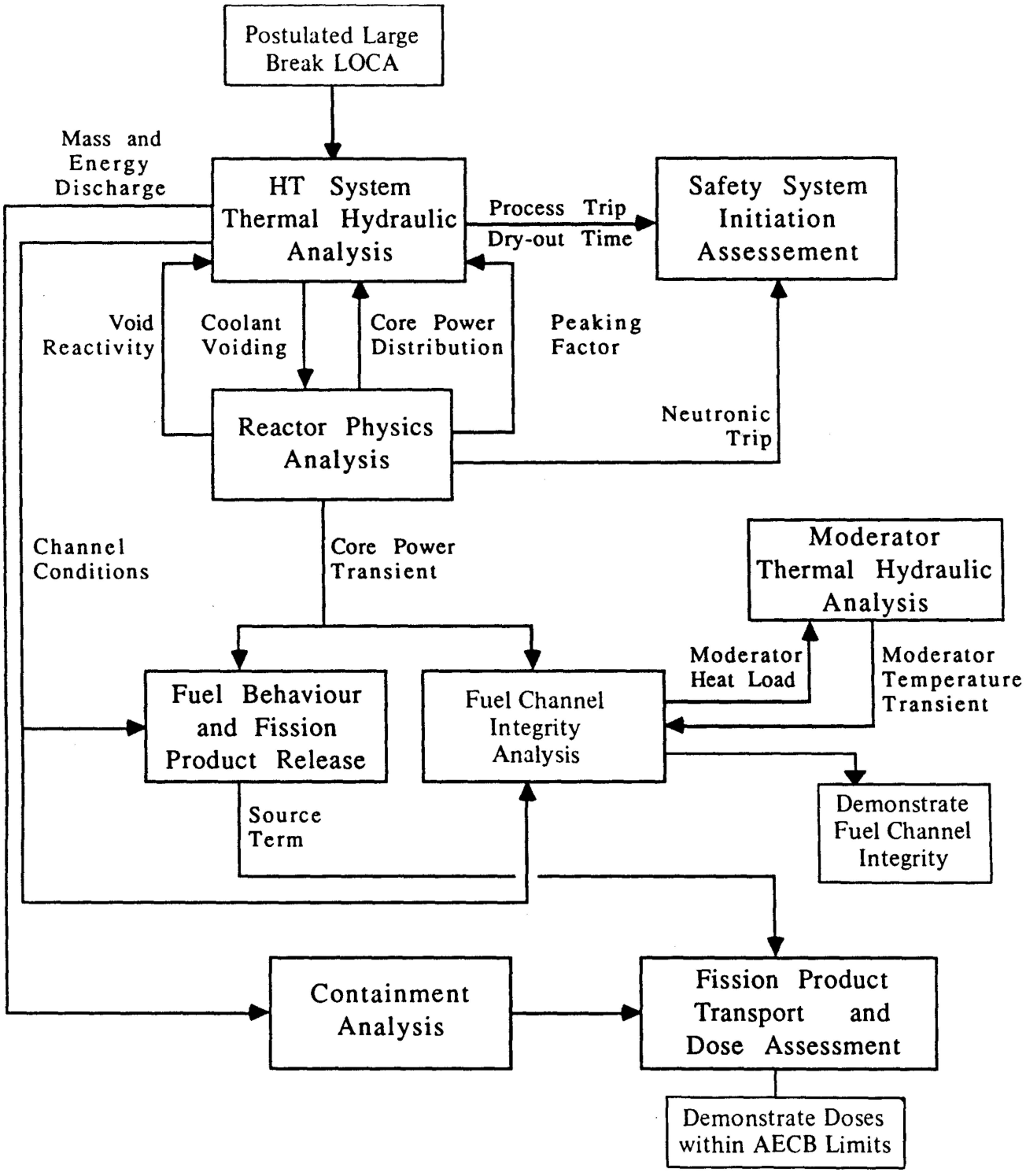

FIGURE 1
Basic Modules Used in LOCA Analysis

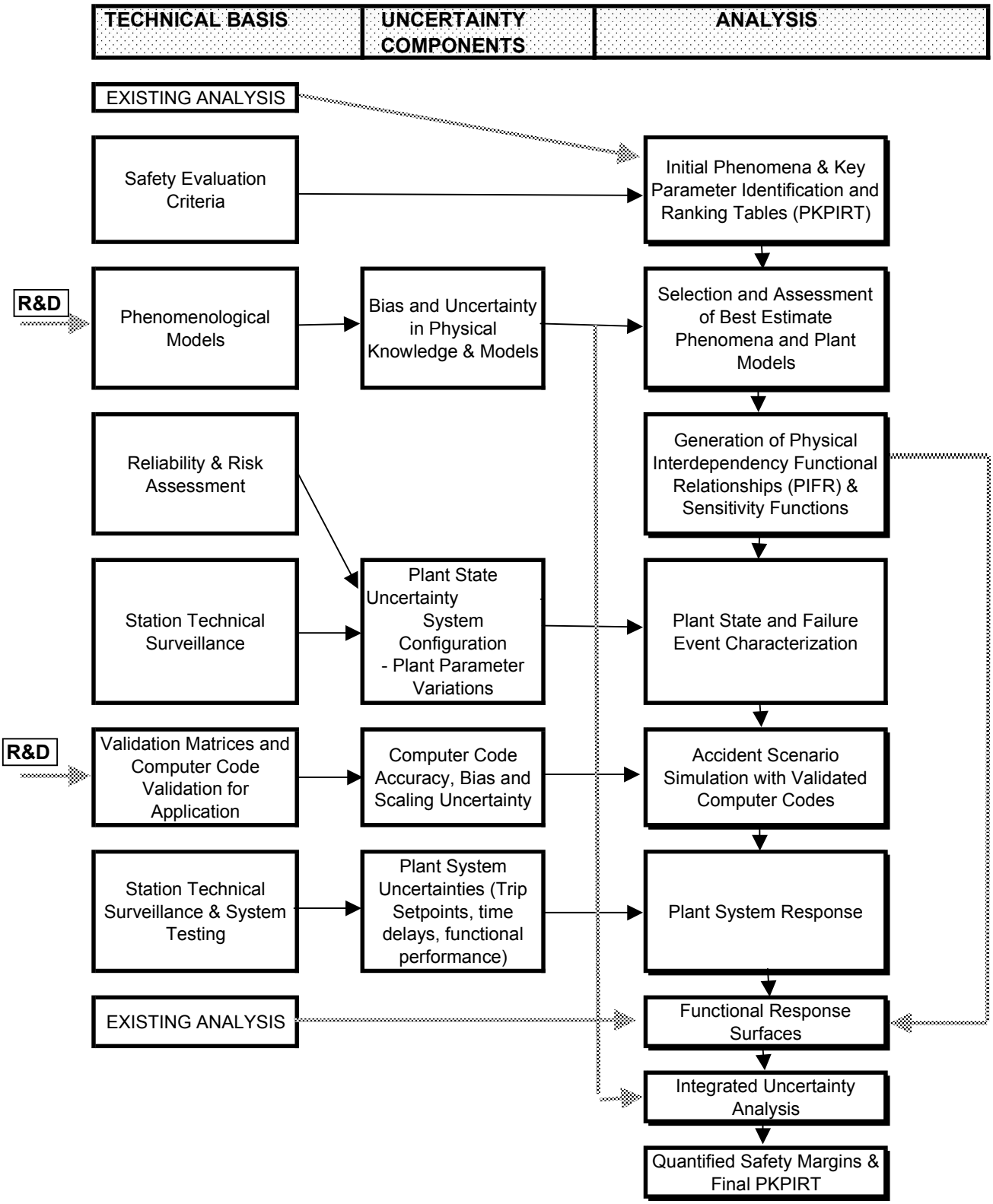

FIGURE 2
ELEMENTS OF OPG's BEST ESTIMATE + UNCERTAINTY METHODOLOGY