Invited at Plenary Session of "Safety Assurance of NPP with VVER", OKB "GIDROPRESS", Podolsk 16-19 May, 2017
ISBN 978-5-94883-147-3 OKB"GIDROPRESS"

Conjugating ALARA, BEPU, Safety Margins and Independent Assessment in Nuclear Reactor Safety

F. D'Auria[1], N. Debrecin[2], H. Glaeser[3]

1 University of Pisa (DESTEC/GRNSPG), Pisa, Italy; 2 University of Zagreb (FER), Zagreb, Croatia; 3 Consultant, Eching, Germany

ABSTRACT

ALARA (As-Low-As-Reasonably-Achievable) is an early principle in Nuclear Reactor Safety, NRS (Nuclear Reactor Safety): Designers and Operators must do their best to minimize doses to the humans. BEPU (Best Estimate Plus Uncertainty) is an approach in Accident Analysis, part of NRS: one may state that BEPU implies the best use of computational tools to determine the safety of nuclear installations. Then, ALARA may be seen at the origin of BEPU, or ALARA is at the origin of BEPU. Furthermore, BEPU (and BEPU elements like V & V, Scaling, procedures of code application and code coupling, etc.) can be extended to all analytical parts of the Final Safety Analysis Report (FSAR). This brings to BEPU-FSAR. Safety Margin (SM) is an established concept in NRS: a few dozen SM values must be calculated in current safety analyses and demonstrated to be acceptable. The SM concept can be extended to everything part of the design, the operation and the environment for a Nuclear Power Plant (NPP) Unit. Here the environment includes the personnel in charge of activities connected with the NPP. The Extended SM concept, E-SM, implies the formulation of some ten-thousands SM values, which shall correspond to a similar number of monitored variables. Reasons for E-SM are the examples in section 4.1. Independent Assessment (IA) is an early requirement in NRS: data ownership and system complexity prevented so far a comprehensive application of the requirement. IA analyses conflict with industry policies to keep proprietary data. IA based BEPU-FSAR analyses are essential to finalize the E-SM design.

In the paper we discuss that: a) ALARA is at the origin of BEPU; b) BEPU-FSAR analyses are the natural origin of E-SM values; c) The implementation of E-SM equals to introducing an additional physical barrier against the release of fission products.

1. INTRODUCTION

Nuclear Reactor Safety constitutes a well-established technology at the time of writing this paper. About five-hundred Nuclear Power Plant units have been operated since the demonstration of the capability to control the fission reaction. A much larger number of reactors (a few thousands) have been constructed and successfully operated for purposes different from electricity production including research and production reactors as well as reactors used for marine propulsion. Accidents occurred, including a few catastrophic ones which severely impacted the exploitation of the nuclear technology.

Two paradoxical situations can be identified for NRS: first, maturity was achieved at a time when the number of NPP units commissioned-constructed per year sharply dropped mainly as a consequence of the

accidents in Three Mile Island (TMI-2) and in Chernobyl; second, industrial interest in implementing research findings and new ideas after those events declined leading to a sort of misalignment between technological capabilities and implementation status. Furthermore, human factors are part of NRS and had a key role in the evolution of the occurred nuclear catastrophes: these are marginally or indirectly considered hereafter.

Concepts and principles in NRS were proposed by those pioneers who developed the nuclear technology in the middle of the past century and since then are embedded into any step of the process leading to electricity production. Those concepts and principles were adopted by other technologies later on and, still today, appear unsurpassed. The implementation of those concepts and principles shall follow the progress in understanding and the development of new techniques.

The starting point for the proposal formulated in the present paper is the growth in knowledge in nuclear thermal-hydraulics during the last three decades of the previous century, noticeably including application to the accident analysis in NPP. Accomplishments like validation of numerical tools, characterization of errors in computation or uncertainty quantification and addressing the scaling issue were established and formed the Best Estimate Plus Uncertainty (BEPU) approach.

BEPU constitutes an established approach for the consistent application of system thermal-hydraulics codes within the licensing process of NPP. This has been developed within the framework of the Accident Analysis part of the Deterministic Safety Assessment (DSA); more insights are provided in the paper. In addition attempts have been made even by international institutions to merge the DSA developed BEPU approach with Probabilistic Safety Assessment (PSA). The first example is constituted by the SMAP and the follow-up SM2A activities performed by the Committee on the Safety of Nuclear Installations (CSNI, part of Nuclear Energy Agency, NEA, within the Organization for Economic Development, OECD), i.e. Zimmermann, 2011: when performing those activities, fault sequences and parameters are not enveloped or bounded; rather, the transients are analyzed using a BEPU approach and discarding of events in the Event Tree (ET) is avoided as far as practicable. The second example is the ASAMPSA project within the European Commission (EC), EC-EURATOM, 2013: in this case the BEPU quality was proposed for PSA level 2 calculations and evaluation of consequences. The third was the follow-up of activities performed within the International Atomic Energy Agency (IAEA): it aimed, see e.g. Dusic et al., 2014, to the integration of DSA and PSA activities making reference to the so-called risk-informed regulation and to the ‘option-4’ to perform NRS analyses.

All those attempts are valuable and shall be considered as background other than providing inspiration for the development proposed in the present paper. The following is also noted:

a) The As-Low-As-Reasonably-Achievable (ALARA) principle, proposed for bounding the radiation impact upon the humans, is consistent with the practice of best use of existing information, i.e. a feature of BEPU, D’Auria, 2017.
b) The methods and the procedures which are part of BEPU can be extended to any sector of NRS where analytical processes are adopted, Menzel et al., 2015.
c) The safety of NPP is expressed in terms of Safety Margins (SM), i.e., for an assigned parameter, the difference between the imposed threshold and the current value which characterizes the system (the NPP in the present case) status. BEPU is the best way to estimate the current value and then the SM value. The actual SM space can be extended, i.e. introducing the E-SM development, D’Auria et al., 2015, covering each logical process within NRS.

d) Independent Assessment (IA) is an early requirement in NRS: however, the needs derived from industrial property and the sophistication of NPP may prevent its implementation, D'Auria & Debrecin, 2014.

The objective for the present paper is to consider as cornerstone elements the ones listed at items a) to d) and to derive a new vision for NRS. The end result is the creation of a barrier to the release of fission products which is in addition to those constituted by clad, pressure boundary and containment. The new barrier has a dynamic nature and a financial worth close to 1% of the value of one NPP unit; the installation of this barrier would have prevented severe evolution of TMI-2 and Chernobyl-4 accidents and, possibly, of Fukushima-1 to -4, under proper circumstances.

2. THE CONCERNED PRINCIPLES, CONCEPTS AND REQUIREMENTS IN NUCLEAR REACTOR SAFETY

The dream to synthesize NRS in a paper is not pursued in the paper. However, a skeleton interpretation is provided which may guide through the logical path followed to link principles, concepts, requirements and outcomes from analyses including the proposal for devoted hardware.

The Nuclear Reactor Safety Technology may be perceived as entailing two main parts, the Fundamentals and the Application, Fig. 1. An idea of the complexity of the matter can be derived from IAEA, 2000, 2006 and 2009.

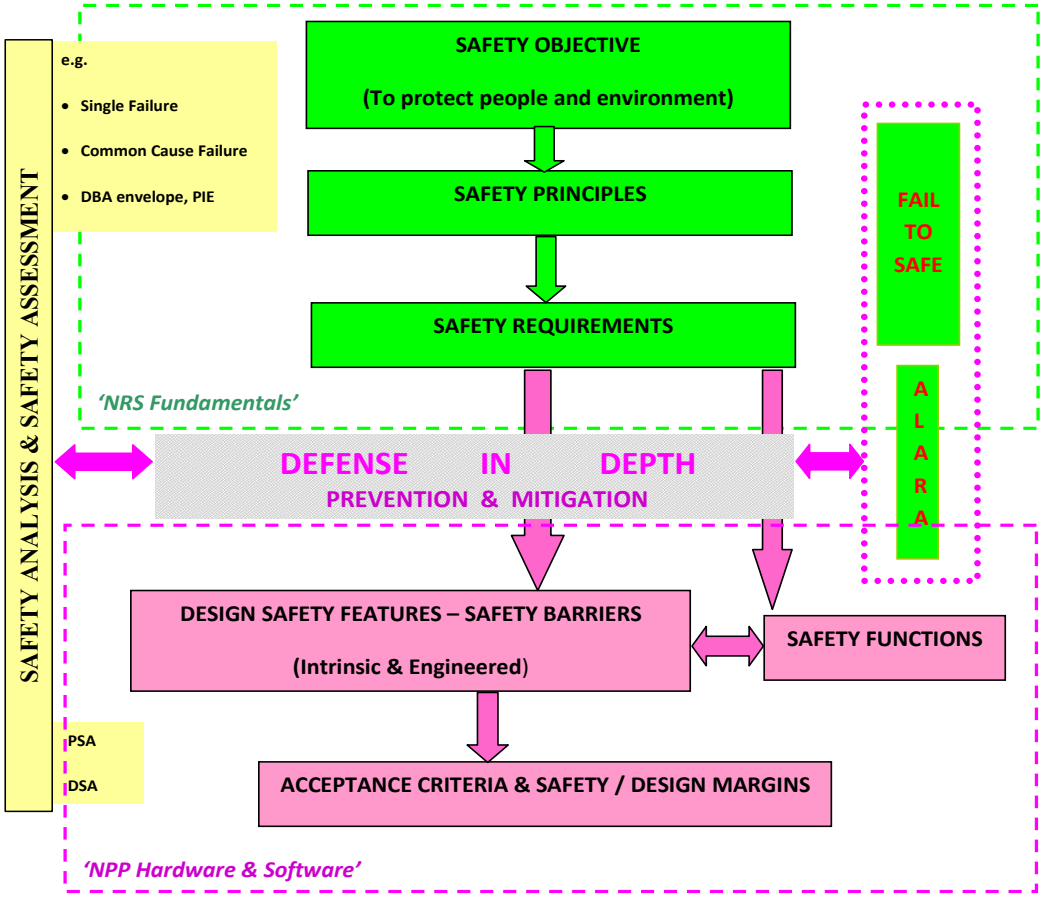

Fig. 1 – Simplified sketch for Nuclear Reactor Safety

The Fundamentals in Fig. 1 include the key safety objective, i.e. to protect people and environment from ionizing radiations, and the related safety principles and safety requirements according to established IAEA nomenclature. The Application makes reference to whatever is done for the design, the licensing (e.g. see IAEA, 2000), the construction, the displacement, the operation and the decommissioning of any nuclear installation involving the presence of radioactive material. Hereafter specific reference is made to NPP equipped with water-cooled reactors.

The bases and the procedures which constitute the established Defense in Depth (DiD) framework shall be seen as the link between NRS Fundamentals and Application. Prevention and Mitigation shall be distinguished in this connection and DiD procedures apply in relation to both.

The design, construction and operation of any nuclear facility, noticeably a NPP, implies the existence of a process within NRS originated by the safety objective. Acceptable safety and/or design margins shall be demonstrated for each step of the process in compliance with the safety Fundamentals. The safety margins imply the reference to acceptance criteria which are established by devoted institutions, typically Regulatory Authority in the Country where the facility is installed. Principles like Fail-to-Safe and As-Low-As-Reasonably-Achievable are part of the overall picture.

The accomplishment of safety fundamentals in the NPP design is demonstrated by safety analysis and assessment. Parameters characterizing the pink blocks part of the NPP Hardware & Software are object of calculations performed within the context of Deterministic Safety Analysis (DSA) and Probabilistic Safety Analysis (PSA). Then, the safety functions are ensuring the integrity of the safety features and barriers. Prevention and mitigation shall be considered as key elements of the Defense in Depth.

A comprehensive Safety Analysis Report (also known as Final Safety Analysis Report, FSAR) for an individual NPP provides the demonstration that the safety objective is met and, noticeably, that acceptable values for SM exist.

2.1 The ALARA principle

ALARA, according to USNRC (Code of Federal Regulation, title 10, part 20 – Standards for Protection against Radiation) means "*making every reasonable effort to maintain exposures to radiation as far below the dose limits in this part as is practical consistent with the purpose for which the licensed activity is undertaken, taking into account the state of technology, the economics of improvements in relation to state of technology, the economics of improvements in relation to benefits to the public health and safety, and other societal and socioeconomic considerations, and in relation to utilization of nuclear energy and licensed materials in the public interest*". The close connection with 'Radiation' and with 'the state of technology' shall be noted.

2.2 The Safety Margin concept and the E-SM

The safety margin for nuclear reactors is defined as the difference or the ratio in physical units between the limiting value of an assigned parameter (typically, the threshold value for the connected acceptance criterion) the surpassing of which leads to the failure of a system or component, and the actual value of that parameter during the life of the plant.

The existence of suitable margins ensures that nuclear reactors operate safely in all circumstances during their life. Sample safety margins relate to physical barriers designed to protect against the release of radioactive material, such as fuel matrix and fuel cladding (typical limiting values are associated with Departure from Nucleate Boiling Ratio [DNBR], fuel temperature, fuel enthalpy, clad temperature, clad

strain, clad oxidation), to reactor coolant system boundary (pressure, stress and material conditions related values), to containment (e.g. pressure and temperature) and to dose to the public being close or far from the NPP.

The accident phenomenology and the related timing are estimated as complete as necessary within the DSA framework. In turn, the PSA approach allows demonstration of the completeness of the set of different scenarios and best estimate methods. The concepts of safety margins and of quantifying changes in safety margins appear as key components of the discussions for modifications in plant design parameters and operational conditions. This includes, for example, power up-rates, life extensions, use of mixed oxide fuels, different cladding materials, design and operation of passive systems and changes to technical specifications. Those modifications impact safety margins in deterministic analyses, while others impact the reliability of systems and components, and yet others impact safety margins and reliability simultaneously.

The concepts of 'Safety Margin (SM)' and 'Design Margin (DM)' are characterized from well-established Fig. 2. The concepts 'Safety Limits' and 'Licensing Margins' are also relevant here.

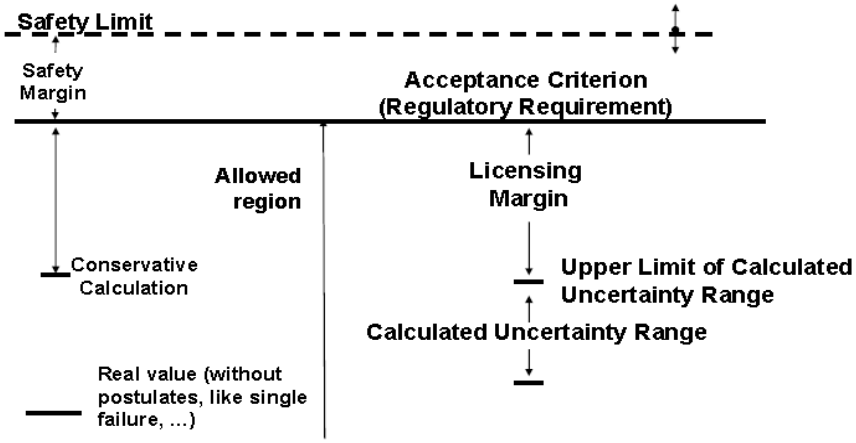

Fig. 2 – Acceptance Criteria, Licensing & Safety / Design Margins and connection with Safety Limits and results of Safety Assessment calculations.

The concepts of SM and DM are expected to be introduced in relation to the following topics (minimum list, to be taken as example and excluding security related issues):

- the control of the 'nuclear chain reaction';
- the amount of 'radioactive source';
- the 'likelihood of an accident';
- the prevention of (each among several) 'failures' of systems and components;
- the prevention of (each among several) 'possibility of escalation' of any off-normal condition of operation;
- defending (each among several) the Barriers and the Safety Features (see below) introduced 'to prevent loss of radioactivity'.

2.2.1 The multi-dimensional space to evaluate E-SM

The DSA and PSA approaches have been developed rather independently from each other. This poses the problem of consistent integration. Hence, a generalization of the concept of safety margin may be beneficial. This shall be given within a multidimensional space. The multidimensional space implies a multi-

face concept, because of the many design-safety-licensing involved aspects, and a multi-field concept, because of the many involved technological fields covering nuclear reactor safety and design.

The multidimensional space can be defined for SM, noting that risk space shall be taken as synonymous of safety space. The key dimensions for the space embracing the definition of SM can be defined as:

A) The key elements characterizing NRS.

B) The technological sectors or the key scientific disciplines of NRS and NPP design and operation.

C) The systems, the sub-systems and the components which constitute the NPP.

D) The time spans which form the life of the NPP.

Human factors shall be considered as part of any of the 'dimensions' above. Key elements are defined for each dimension hereafter:

A1) Safety Principles, i.e. SP-1 to SP-10, i.e. according to established document (e.g. IAEA framework).

A2) DiD Levels, i.e. DL-1 to DL-5, i.e. according to established document (e.g. IAEA framework).

A3) Safety Barriers, i.e. SB-1 to SB-6, i.e. according to established document (e.g. IAEA framework).

A4) Safety Functions, i.e.SF-1 to SF-19, i.e. according to established document (e.g. IAEA framework).

A5) PSA Elements, i.e. PE-1 to PE-n, i.e. according to results of BEPU-based safety analysis (see below).

A6) DSA Elements, i.e. DE-1 to DE-m, i.e. according to results of BEPU-based safety analysis (see below).

The values 'm' and 'n' shall be associated with the results and the procedures of the applicable DSA and PSA.

B1) Radio-Protection;

B2) Thermal-Hydraulics;

B3) Structural Mechanics;

B4) Neutron Physics;

B5) Civil & Electrical Engineering.

An attempt is made to minimize the number of disciplines. Several SM and DM are expected in relation to each discipline.

C1) Reactor Pressure Vessel (RPV);

C2) Reactor Coolant System (RCS) piping;

C3) Balance of Plant (BOP) piping;

C4) Core;

C5) Core components;

C6) RPV components except core;

C7) RCS components;

C8) BOP components;

C9) Containment;

C10) Containment components;

C11) Core components;

C12) Reactor building;

C13) Auxiliary buildings;

C14) Reactor building and auxiliary building components;

C15) Site (parameters);

C16) Site structures and components;

C17) Off-site (NPP related relevant parameters);

C18) Off-site structures and components (NPP related);

C19) Instrumentation and Control (I & C) .

The value '19' associated to the identification of systems, sub-systems and component of the NPP is somewhat arbitrary. Modification in this number will not affect the procedure. Furthermore, each of the listed items should be intended as Ci-j where 'i' ranges between 1 and 19 (present proposal) and 'j' can assume any value connected with the level of detail of the analysis.

D1) Site selection;

D2) NPP design;

D3) NPP construction;

D4) NPP licensing;

D5) NPP operation;

D6) NPP maintenance;

D7) NPP decommissioning.

The items from D1) to D7) should be considered as an outcome of the established knowledge of NRS and NPP technologies.

Thirty-five (35) E-SM tables are generated which constitute the multidimensional E-SM matrix, IAEA, 2015. The use of the matrix can be explained with the help of the sketch in Fig. 3. The figure has been obtained assuming non-dimensional E-SM definition related to non-dimensional acceptance criteria which are set at the unity value. In relation to each safety barrier and safety function, 'n' E-SM values can be defined. Furthermore, one average E-SM can be created per each safety barrier and each safety function. Finally, one average E-SM can be created as a function of time per each NPP, specifically following any modification or any (relevant) operational event.

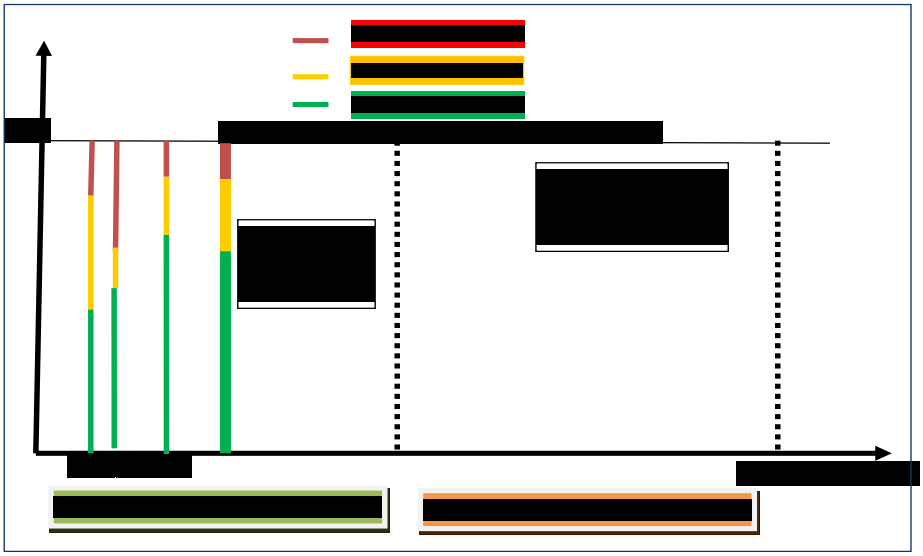

Fig. 3 – Application of the E-SM matrix.

A number of 'new' detectors of the order of 10^4 is expected to be installed for continuously monitoring the safety margins part of the E-SM matrix. Examples of measured quantities include the stem position of all valves and those quantities which are the result of BEPU-FSAR analyses (see below); examples of detectors are cameras installed along various circles around the NPP unit.

The application of the procedure according to the diagram in Fig. 3 also requires establishing the ranges 'safe', 'acceptable' and 'close to the limit'. Once this is completed, the objective safety status for the concerned NPP can be evaluated at each instant of the life.

2.3 The Independent Assessment requirement

The legal branch of NRS is known as licensing. A licensing process is initiated each time the construction is planned of a new nuclear installation where radioactive material is present. The licensing process aims at ensuring the safety of each NPP unit, as well as at protecting the public and the environment from harmful radiations. A Government Body under the control of a Ministry, typically Industry or Safety-Security Ministry, is responsible for the licensing process and dictates the modalities which (typically) are part of the Atomic Energy Act and of the Laws. The Government Body is known as licensor. The licensor must approve the safety demonstration prior to the start of the operation of a facility. On the other side, there is the owner of the nuclear installation or facility, which is, typically, the operator of the concerned NPP unit or the applicant of the licensing process. The operator is known as licensee. The operator must fulfill all the obligations set by the licensor, namely making available any information detail and data related to the facility.

In between the licensor and the licensee, there are typically other organizations, or institutions, or individuals: examples are the NPP designer and vendor, consultants including technical support organizations and research bodies including universities. Those 'other organizations' cooperate either with the licensor or with the licensee to finalize the licensing process.

Looking at the above terms the licensing process constitutes a perfect process and there is no room for improvement. However, in order to undermine the concept of perfect process, also showing its complexities, let's consider the following facts (just three out of more possible examples):

a) In order to demonstrate the safety of NPP, analysts need to calculate temperature and stresses in individual fuel pins (thickness of the clad is few tenths of mm) solving a multi-scales and multi-physics problem; providing an analogy in aeronautics, the given problem is similar to demonstrate the integrity of a crystal glass glued on the wing of an airliner following a cycle take-off / trip under any meteorological condition / landing.

b) There is evidently no countermeasure for the falling of a meteorite upon a nuclear facility. The falling in the region around the facility may also generate earthquake and tsunami beyond the design limits of the facility. The issue here is that the probability value for meteorite falling may have changed (i.e. because of new evidence became available) after the facility has been put in operation.

c) Most of the NPP units now in operation have been designed at a time when computers and computational tools and methods were not available. The obvious question arises on how the new findings can be integrated in the old designs.

Furthermore, it is part of the human nature to optimize any aspect, which may generate a benefit: this is the basis of progress of civilization. Therefore, designers continuously improve the system and regulators continuously improve the techniques to check the design. Independent assessment (IA), i.e. the safety evaluation made by licensor knowing the construction data of the facility and adopting methods 'independent' of the licensee, constitutes the foundation of the licensing process (USNRC, Code of Federal Regulation, title 10).

So, where is the weakness?

In the attempt to address the question, two items are considered:

- Modifications introduced by industry are not always and systematically requested by regulators for the independent assessment: in the given example, the type of glue used to attach the glass to the wing may produce unexpected effects.
- New analytical techniques and related capabilities as well as new evidence are not necessarily used in the analyses by regulators and by the industry; for instance any impact in safety demonstration is calculated from the change in probability of a meteorite fall.

The experience gained in a recently completed effort to demonstrate the safety of an NPP in parallel to the safety demonstration provided by the designer helped in answering the question "Where is the weakness?" The concerned effort is the licensing process of Atucha-2 in Argentina. A 'vendor-independent' safety analysis was needed including accident analysis. The new safety evaluation was completed and approved by the licensor. The facility detailed construction data and the latest computational techniques (available thirty years after the time of design of the facility) were adopted: this implied, among the other things, the use of the BEPU approach (section 3), e.g. D'Auria et al., 2012, and the design and operation of an experimental facility, Moretti et al., 2016.

The diagram in Fig. 4 is taken from the effort to prepare the IA based Final Safety Analysis Report (FSAR) for Atucha-2, D'Auria et al., 2012a.

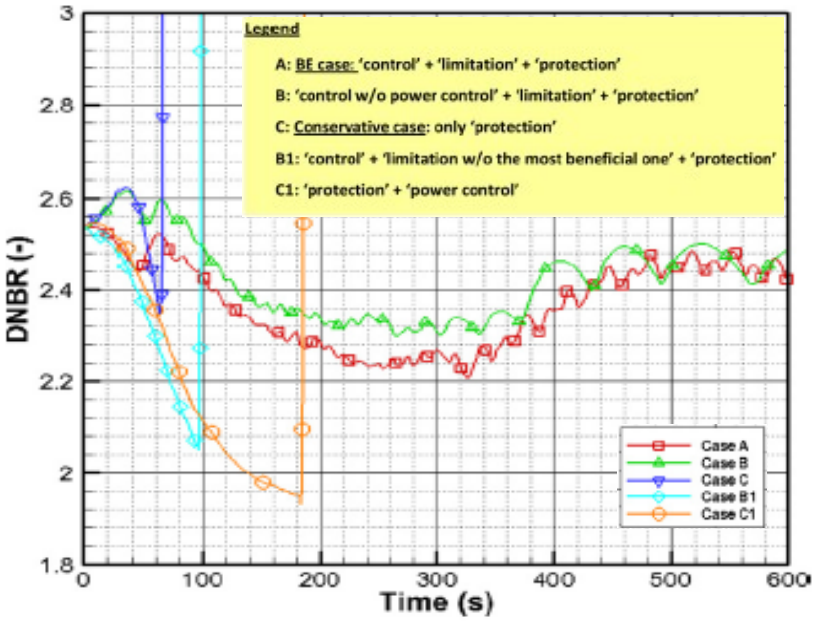

Fig. 4 - Results from AOO (Anticipated Operational Occurrence) analysis of Atucha-2: DNBR reported for Cases A, B, C, B1 and C1 as a function of time.

IA brought to the need to simulate all details of the Instrumentation and Control (I & C) system of the facility. The simulation of I & C demonstrated that results of conservative assumptions may not be conservative; the lowest value for DNBR was achieved when a number of components successfully operate. The I & C systems are (correctly) designed to keep full power following minor perturbations; however, they keep the potential to bring the NPP status far away from the standard operational conditions, thus opening for accident scenarios different from the one terminated by early scram under conservative assumptions (blue line, or Case C in Fig. 4).

3. THE BEPU APPROACH

On the one side, it is straightforward to discuss the outcomes of a BEPU calculation; on the other side it is difficult to explain what the procedure to obtain BEPU is. Hereafter some generic BEPU-definitions are given, D'Auria, 2017, and 2017a:

- BEPU is a logical process or an approach which connects the understanding in nuclear reactor safety (see also licensing below) with nuclear thermal-hydraulics.
- The starting point for BEPU is the understanding of the phenomena. Thus, BEPU implies the identification of the accident scenarios which are part of the 'design basis envelope'.
- BEPU implies the existence of qualified computational tools including numerical codes dealing with different disciplines, input decks or nodalizations and a method to evaluate the uncertainty. The words 'different disciplines' imply the coupling among codes and the ability to qualify the resulting coupled codes.

- BEPU needs the existence of qualified procedures for the application of the computational tools.
- BEPU needs qualified code users and experts capable of evaluating the results and of establishing whether additional analyses are needed.
- BEPU needs the existence of 'legal' acceptance criteria (e.g. suitable licensing framework).
- The application of BEPU implies the deep knowledge of the licensing process in the Country where the nuclear power plant will be installed and in the Country where the same plant has been designed. Furthermore, advancements in licensing process by different international institutions shall be continuously considered.
- The structure of the FSAR must be adapted to BEPU and connections shall be identified among different chapters (see section 3.1 below): this is specifically true in relation to the design of the core, the experimental data drawn during the commissioning period of the plant and the design of operational and emergency procedures.
- Any BEPU report as well as any BEPU finding should be a living document, periodically updated.

The basic key elements of BEPU are:

- ✓ Verification and Validation, V & V, for system codes, Glaeser, 2017.
- ✓ Scaling in nuclear thermal-hydraulics, OECD/NEA/CSNI, 2017.
- ✓ Code coupling, OECD/NEA, 2004.
- ✓ Uncertainty methods and qualification, IAEA, 2008 and Glaeser, 2017.

A summary-outline of the technological background identified by the listed references is already beyond the scope for the paper. Rather a few graphical representations are used to provide a look into the BEPU technology: 1) historical framework for BEPU; 2) coverage of accident analysis by BEPU; 3) breaking the barrier between PSA and DSA; 4) the BEPU database. These are given in Figures 5 to 8, respectively.

Figure 5 shows a five decades background history for BEPU; details can be found in D'Auria, 2012. USNRC (Atomic Energy Commission, AEC, at the time) proposed the Interim Acceptance Criteria in 1971 for the design of Emergency Core Cooling Systems, ECCS. Remarkable achievements in the area of V & V came from OECD/NEA/CSNI activities in the 80's also documented in a compendium of research by USNRC. The Code Scaling, Applicability and Uncertainty (CSAU) effort preceded Uncertainty Method based on Accuracy Extrapolation (UMAE) and the statistical method based on Wilks' formula first proposed by GRS in Germany. At the regulatory level, interpretations for performing accident analyses were proposed in the early 90's and middle 00's by USNRC, Regulatory Guide RG-1.157 and RG-1.203, respectively. The documents IAEA, 2008 and IAEA, 2010, also identify guidelines for the application of BEPU. At the level of demonstrating the capability of methods: a) the UMS project dealing with applicability of uncertainty methods was completed in the middle of 90's; b) the capability to deal with the Internal Assessment of Uncertainty (IAU), i.e. to consider the deviation of a calculation compared with an experiment as an intrinsic feature of the code that generates the calculation, was demonstrated in the year 2000 (application of the CIAU method, or the Code with capability of IAU); c) the BEMUSE project to demonstrate the qualification of uncertainty methods was completed towards the end of 00's. At the level of application, cornerstone activities were performed around 2000 and 2010, dealing with the application of BEPU to the analysis of Large Break Loss of Coolant for the licensing of the Angra-2 NPP in Brazil and of all accidents part of the FSAR Chapter 15 for the licensing of the Atucha-2 NPP in Argentina. A number of other applications of BEPU are mentioned by Glaeser, 2017.

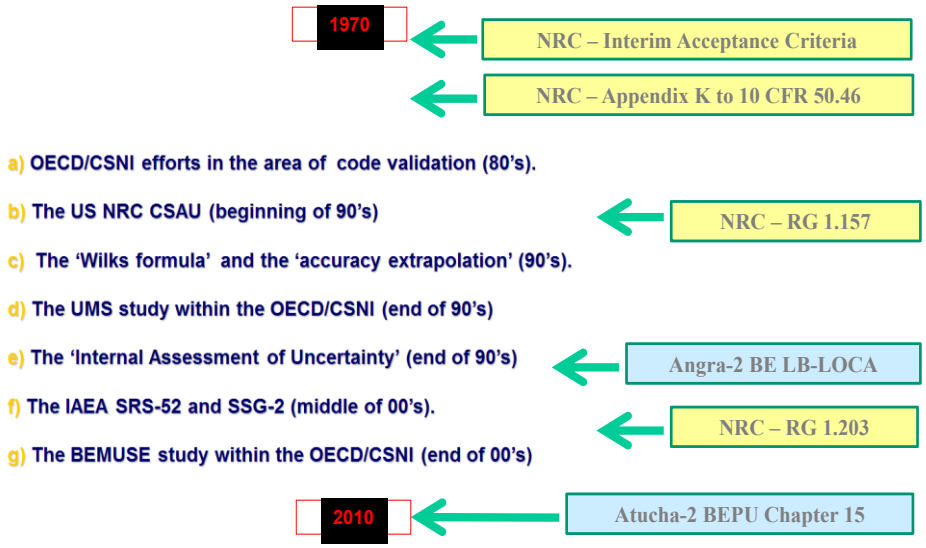

Fig. 5 – A historical framework for BEPU.

Figure 6 shows the applicability range for BEPU within the domain of accidents analysis with accidents having different severity. Accident Management area can be concerned until the situation of the core keeping a coolable geometry. The rigor of computational tools including the V & V procedures and the uncertainty methods cannot be kept in situations of degraded core, i.e. Severe Accident with Core Damage (CD) and Large Releases (LR). On the contrary, the 'regions' of control systems and safety systems are BEPU regions. Cross-links between BEPU region and PSA region can be derived from the reported sketch.

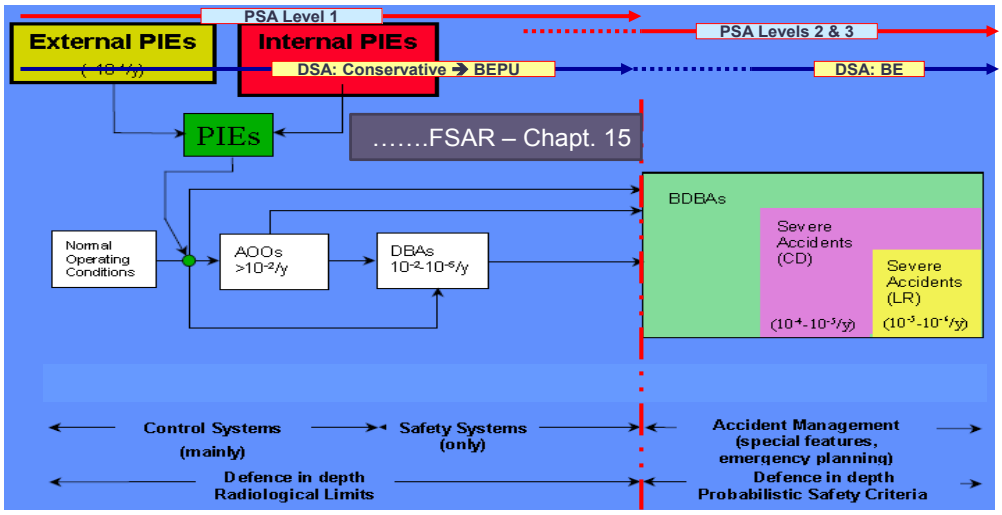

Fig. 6 – BEPU connection with risk informed accident analysis *(J. Misak and M. Dusic largely contributed to this sketch)*.

Making reference to Fig. 7, similar elements may be used to characterize both DSA and PSA pyramids, e.g. LOCA, Anticipated Transient Without Scram (ATWS) and Station Blackout (SBO). In the same sketch, Global (Safety) Margins and Core Damage Frequency (CDF) are put at the top of the pyramids, while, accident scenarios on the left side correspond to Fault Tree (FT), Event Tree (ET) and Human Reliability Analyses

(HRA) on the right side. Uncertainties characterize both DSA and PSA approaches (bottom of the pyramids). Performing a consistent risk informed BEPU application implies breaking the barrier between DSA and PSA.

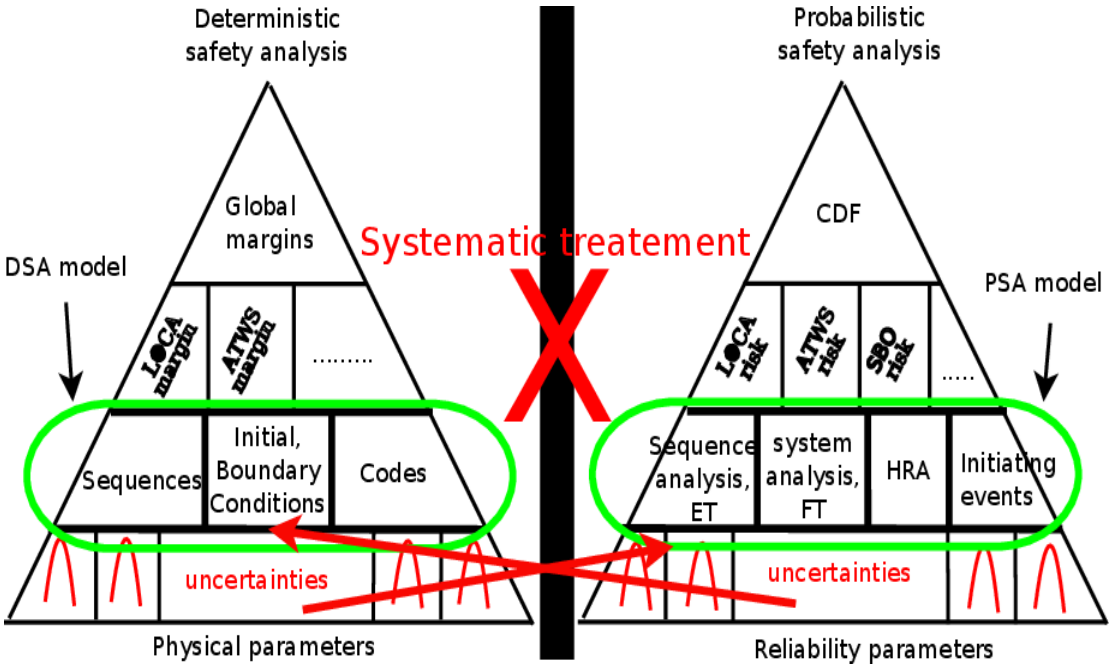

Fig. 7 – Risk informed BEPU approach breaking the barrier between DSA and PSA.

The Fig. 8 shows that databases having various origins are needed for the application of the risk informed BEPU approach. The word 'database' shall be intended as part of the knowledge management and of the demonstration of the expertise needed; for instance, qualification of computational tools and of analysts shall be performed using suitable data; reference data (the 'best' available) are needed to perform PSA applications.

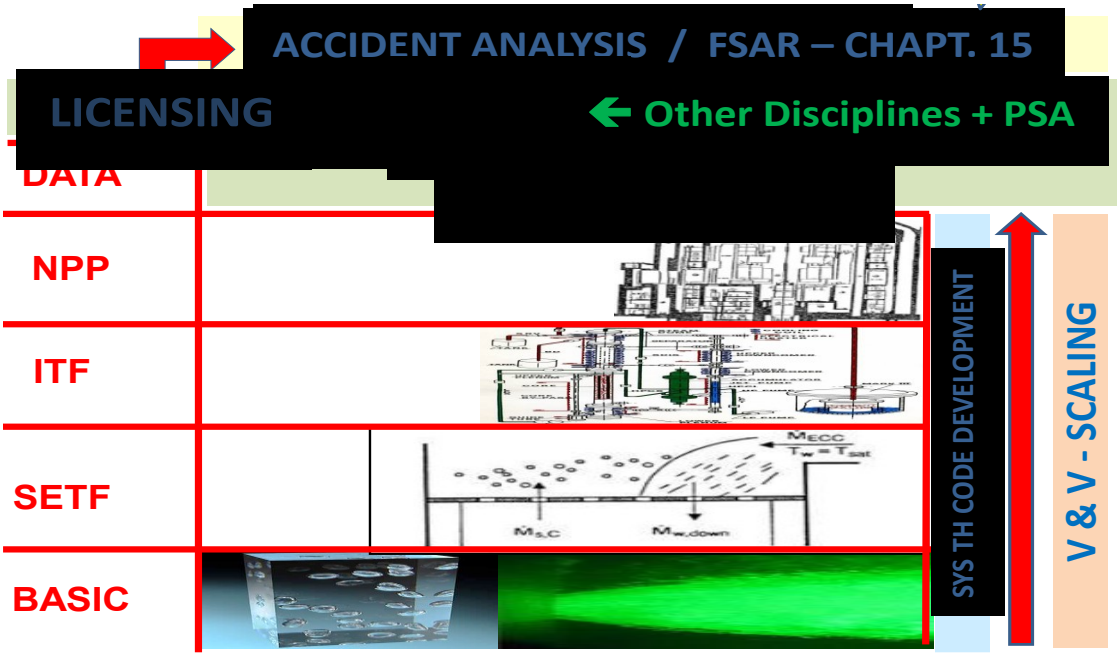

Fig. 8 – The database for BEPU.

3.1 The BEPU-FSAR

Industrial applications of BEPU are limited to the area of accident analysis in NRS, see also Fig. 5. The feasibility of the application of BEPU methods to any area of NRS where analytical techniques are used has been recently investigated, Menzel et al., 2015 and 2016. A systematic overview of the content of the FSAR allowed the characterization of a list of 'key disciplines' and related computational tools. The proposed idea is to apply BEPU methods to each step of FSAR, i.e. creating the BEPU-FSAR.

The possible exploitation of the BEPU-FSAR requires an industrial and/or applied R & D effort beyond the boundaries of the activities performed so far (i.e. cited references and present paper). However, the following benefits are expected from the implementation:

- To make uniform the quality of analyses throughout FSAR: for instance, quality of database and computational tools and related impact upon consequential uncertainties in the safety evaluation shall be the consistent for:
    a) demonstrating the compliance of civil structures with requirements,
    b) calculating the probability and the consequence of Postulated Initiating Events (PIE) including external events, see Fig. 6,
    c) performing accident analysis, i.e. a situation where BEPU is applied and the environment where BEPU is developed.
- To break the barriers between 'neighboring' disciplines relevant to design and safety evaluation for NPP (i.e. in addition to breaking the barrier between DSA and PSA already discussed). For instance, should an earthquake occur, propagation of waves into ground, soil structure interaction, influence of close structures on the site, loads on mechanical structures like containment and pressure boundary for Reactor Coolant System, possible pipe break and consequential missile generation, jet thrust, jet impingement, pipe whip are all treated step-by-step and separately. Current (BE) computational technology allows an integrated approach where actual feedbacks are modeled.
- To introduce a rationale for the classification of the safety importance of systems, components and structures. In other terms, the current quality classification should be based upon BE analyses which take into account continuously advancing boundary of knowledge, the lifetime of those systems and components and the actual timing of an event: for instance a system which is unimportant for safety during nominal operating conditions may become of outmost importance because of (minor) failures occurred during a concerned transient.
- To contribute to the objective of a uniform qualification level for personnel involved with the NPP, design construction and operation. BEPU procedures can be used to qualify technicians working in different sectors of nuclear technology. BEPU techniques may help in fixing homogeneous criteria for training in relation to various NPP related topics, see e.g. the NUTEMA, BEPU based knowledge management facility, D'Auria et al., 2011.
- To evaluate thoroughly the innovation introduced in the design of NPP, namely of systems and components relevant to NRS. One example is constituted by the passive systems: an error in the angle of the axis +/- 1% related to the horizontal plane has no effect in case centrifugal pump drives the flow. The same error may largely affect the performance of a passive system, i.e. Jafari et al., 2003. Calculating the reliability of a passive system implies coupling of methods and data from thermal-hydraulics, structural mechanics, construction techniques and reliability, i.e. the domain of BEPU-FSAR.

❖ To contribute to a systematic and comprehensive identification and classification of the E-SM, as discussed with more details in sections 2.2.1 and 4.1 of the present paper.

4. COMBINING ALARA, BEPU-FSAR, IA AND E-SM

The outlines provided for ALARA, SM and E-SM, BEPU and BEPU-FSAR and IA are embraced hereafter in the attempt to identify a worthwhile path in NRS. A humble sketch for the path can be seen in Fig. 9. Related to the elements in the sketch, in addition to the legend, the following statements apply:

- NPP Unit, NRS requirements and FSAR constitute part of established technology not discussed in the paper. Namely FSAR encompasses all elements part of the picture.
- ALARA, BEPU and SM are part of established technology outlined in the paper.
- BEPU-FSAR and E-SM constitute proposals in this paper.
- Independent Assessment (IA) is an established requirement: its implementation, i.e. the impact upon NRS applications, can be largely improved when combined with BEPU and BEPU-FSAR.
- Additional Safety Barrier is an expected outcome discussed in section 4.1.

The connection between IA and BEPU as well as between BEPU and SM has been outlined by D'Auria et al., 2017, and by D'Auria et al., 2017a. Before attempting a connection among all elements, possibly identifying some benefits, the roles of NRS requirements and of FSAR are discussed in advance.

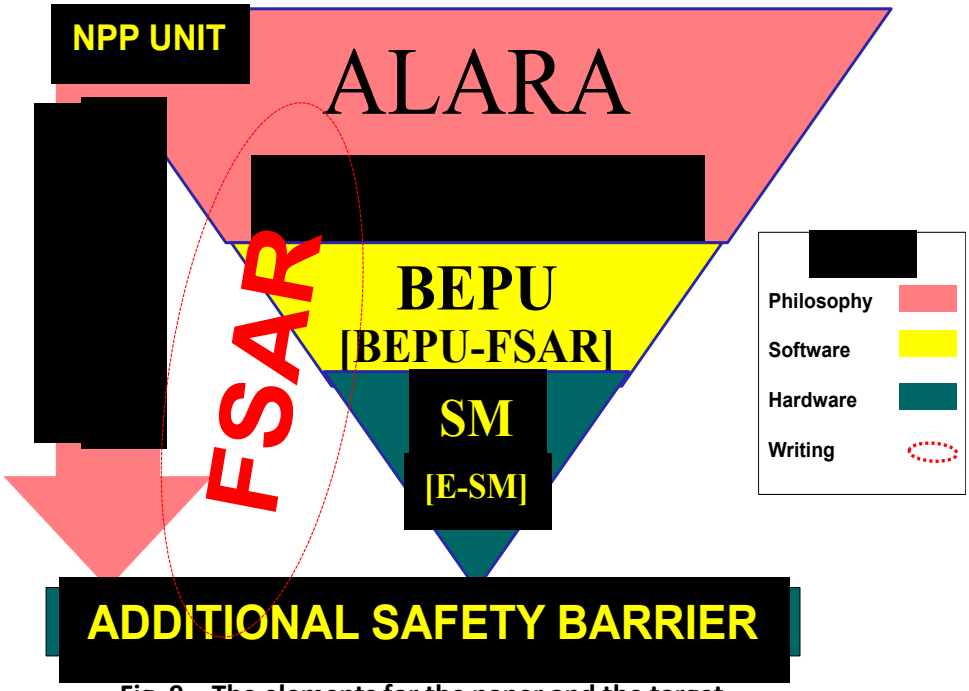

Fig. 9 – The elements for the paper and the target.

NRS requirements are fixed by regulatory authorities (already mentioned). They are considered comprehensive (any related judgement is irrelevant) and do not need major modifications (eventually, any modification shall follow paths which are outside the domain for the paper). The requirements drive any process in NRS: this is the motivation for the presence in the given picture (Fig. 9). FSAR is the compendium of all findings from safety assessment in relation to a single NPP unit. The current structure and list of content of FSAR are considered adequate; however, the amount of detail and the basic methodologies of

the documented results shall be adapted to BEPU. The BEPU-based FSAR will continue to encompass all elements in the picture of Fig. 9.

The following connections are identified.

I) *NPP unit➔ E-SM ➔ Additional Safety Barrier*. The hardware and software of the NPP unit are expected to be modified to accommodate for the monitoring of 'new' SM. The complexity and the value of NPP are realized here and the proposed changes shall have negligible impact upon cost and complexity (see section 4.1 for the additional safety barrier).

II) *ALARA ➔ BEPU*. 'Making every reasonable effort to maintain exposures … as far below the … limits' is translated into 'Utilizing the best available techniques to calculate the exposure'. So BEPU is a consequence of ALARA and delays in exploiting its features are not justified.

III) *BEPU ➔ BEPU-FSAR*. The possibility to perform BEPU analyses of all Design Basis Accidents (DBA) which are part of FSAR has been demonstrated (e.g. D'Auria et al., 2012). The applicability of BEPU methods and procedures like code V & V, scaling, qualification of data and of analysts, to any analytical part of FSAR appears straightforward and is envisaged (e.g. Menzel et al., 2016). BEPU-FSAR appears to be the natural extension of BEPU. However, full demonstration of BEPU-FSAR capability requires resources which are not expected to become available without the engagement of industry which should be convinced in advance of the benefits of the extension.

IV) *BEPU ➔ SM and BEPU-FSAR ➔ E-SM*. Analytical techniques applied to accident analysis can be used to characterize reference conditions for the operation of NPP systems called in operation in nominal and off-nominal situations, including so-called technical specifications (tech-spec) values. This applies to BEPU and to the set of variables connected with the current definition of SM. It appears reasonable to predict that BEPU-FSAR analyses can support the definition process for E-SM and contribute in fixing selected E-SM values.

V) *BEPU➔ IA ➔SM*. In the item above it is clarified that BEPU can be used for the characterization of SM. So what is the role for IA? First, it seems important to state that 'IA is not a process against the owner of data' and that 'IA does not imply the loss of data ownership'. Rather, properly performed IA has the potential to improve a design or the industrial product under concern through the use of procedures and tools not applied for the original design. IA is a requisite for a consistent (independently assessed) set of SM (and E-SM) values and related monitors.

The full chain of elements can be generated:

ALARA➔BEPU (and) **BEPU-FSAR➔IA➔ (SM** and**) E-SM**.

The entire process must comply with NRS requirements and be documented in the FSAR.

4.1 The additional safety barrier

The enemy is the radiation, so the terms Defense-in-Depth (DiD) and Safety Barriers remind us the target to defeat the enemy as stated in relation to the discussion of Fig. 1. At least three safety barriers are commonly identified and are part of current NPP configurations: the Zircaloy fuel clad, the steel pressure boundary for the primary system and the concrete containment. Those barriers have a static nature, however their integrity is ensured by systems also constituted by safety functions which have a dynamic nature and also may adapt to the evolution of possible accident scenarios.

So, what are the needs and the in-principle features for an additional safety barrier? The answer as follows:

- The need for a new barrier should be justified by small cost and large reduction of CDF: although no analysis is performed, target costs and reduction in CDF for the 'new' barrier should be less than 1% the overall cost of one unit and 1-2 orders of magnitude, respectively.
- The new barrier should be physically separated from other barriers and at the same time providing support to the existing barriers (not introducing new failure modes for the overall system): detailed design is needed to confirm the achievement of this goal.

The elements of the 'additional' proposed barrier are:

A) The results of BEPU-FSAR analyses which are continuously updated.
B) The installation and the operation of 10^4 (order of magnitude) devoted transducers.
C) The combination of signals from transducers and the BEPU-FSAR analysis results.
D) The availability of resources corresponding to envisaged needs, e.g. remote core rescue systems and operators, D'Auria et al., 2012b.

Thus, the barrier consists of transducers, computers, computational tools (i.e. for performing analyses and software for data treatment and E-SM derivation) and data (i.e. continuously updated results of analysis and signals from transducers).

The proposed approach has the potential to prevent the occurred nuclear catastrophes. Some examples are given below to clarify the features of the barrier.

Example 1, the first TMI-2 case. Before the occurrence of TMI-2 event, the Pilot Operated Relief Valve (PORV) of pressurizer was leaking and one manual valve in Emergency Feed-Water (EFW) line was closed (should have been open). Leakage from the PORV and EFW line valve are part of monitored E-SM quantities. Individual E-SM values associated with PORV leakage and EFW line valve closed would not cause any action, however the combination of those two E-SM causes 'red signal alarm' and scram. TMI-2 reactor would have been scrammed before the start of the accident.

Example 2, the second TMI-2 case. Assume the undetected PORV stuck open occurrence: this is a hypothetical condition for TMI-2 event because the accident would have not been happened if the additional barrier was installed. One E-SM signal is the temperature in the PORV sump tank. The early detection of PORV stuck open would have prevented any core damage.

Example 3, the Chernobyl case. The misconduct of operators 5-10 hours (various E-SM involved) prior to the explosion would have created various 'red signal alarms' and scram. The zero power situation achieved few minutes before the explosions would have created an '«extreme» red signal alarm' with devoted scram not under the control of the operators. The Chernobyl accident would have not been occurred.

Example 4, the first Fukushima case. The continuously updated BEPU-FSAR analyses would have considered an external PIE including 20 m (or more) tsunami wave, due to recent tsunamis like the Thailand tsunami, not part of the original NPP design. NPP operation would have not been allowed: 'red signal alarm' generated decades before the event.

Example 5, the second Fukushima case. Assume the NPP was in operation under current design parameters at the time of the Sendai earthquake: this is a hypothetical condition for Fukushima because the units would have not been in operation if the additional barrier was installed, or, if they were in operation, new

protection systems against tsunami would have been built. Satellite detection of tsunami wave height, part of E-SM, would have generated an '«extreme» red signal alarm' with request of substitute Emergency Diesel Generators, EDG. Reasonably, EDG would have not been dispatched to the site before the time when wave hit the site, but reasonably it would have been dispatched on time to prevent any core melt.

Example 6, human performance and security case. Let us consider here the event of the airplane crash in the French Alps occurred in 2015. Signals connected with the health of operators (the pilot in this case) and conditions of the cockpit (e.g. one pilot alone in the cockpit) are part of the E-SM. The combination of those two signals would have generated a 'red signal alarm' on time to prevent that tragedy.

5. CONCLUSIONS

The triggering idea for the paper is that NPP technology is stagnant and initiatives shall be undertaken to restore credibility from the public: the alternative is the irreversible decline of the technology. Furthermore:

a) Any step in the NRS demonstration should be based upon analyses and data: this also implies that the fall of a meteorite should be part of the PSA; its probability value should become a target for the Core Damage Frequency (CDF).
b) Consistently with the proposal of pioneers in NRS, technological achievements must be timely evaluated.
c) In relation to Independent Assessment, the industry should address the dilemma 'running the risk of releasing proprietary data' or 'decreasing (maybe down to zero) the probability to build new units'.

BEPU-FSAR and E-SM constitute the two-tier integrated proposal for improving NRS technology. Introducing related findings into NPP design has the potential:

A) to create an additional safety barrier to the release of fission products;
B) to prevent severe accident occurred so far.

A suited cost-risk-benefit analysis is well beyond the constraints of a scientific paper: however one may guess that the cost of the proposed innovation shall be below 1% the cost of one individual NPP and the gain in terms of CDF (per year) shall be 1-2 orders of magnitude.

The proposed additional safety barrier has a dynamic nature, which adapts to the current NPP status, considering the latest available information from technology

Industry and regulators are expected to take profit from the integrated proposal. The acceptance of nuclear plants by the public could also improve following the implementation of independent BEPU-FSAR and E-SM.

REFERENCES

D'Auria F., Muellner N., Martinucci M., Laudazi F., D'Amato R., Tambasco P., 2011, NUTEMA: a tool for supervising nuclear technology and for the transfer of knowledge, J. Nuclear Knowledge Management, Vol. 5, No. 4

D'Auria F., 2012, Perspectives in System Thermal-Hydraulics, J. Nuclear Engineering and Technology, Vol 44, 8, 855-871

D'Auria F., Camargo C., Mazzantini O., 2012, The Best Estimate Plus Uncertainty (BEPU) approach in licensing of current nuclear reactors, J. Nuclear Engineering and Design, Vol. 248, 317-328

D'Auria F., Camargo C., Muellner N., Lanfredini M., Mazzantini O., 2012a, The simulation of I & C in accident analyses of nuclear power plants", J. Nuclear Engineering and Design, Vol. 250, 656-663

D'Auria F., Galassi G., Pla P., Adorni M., 2012b, The Fukushima Event: The Outline and the Technological Background, J. Science and Technology of Nuclear Installations, Vol. 2012, Article ID 507921

D'Auria F., Debrecin N., 2014, Perspectives in Licensing and Nuclear Reactor Safety Technology, Invited at 3rd Int. Scientific and Technical Conference "Innovative Designs and Technologies of Nuclear Power - ISTC NIKIET-2014", Moscow (Ru), October 7-10

D'Auria F., Glaeser H., Kim M-W., 2015, A Vision for Nuclear Reactor Safety, Key-Speaker at 46th Jahrestagung Kerntechnik Annual Meet., Berlin (G), May 5-7

D'Auria F., 2017, Best-Estimate Plus Uncertainty (BEPU) Approach for Accident Analysis, Chapter 14 of Book 'Thermal-hydraulics of Water Cooled Nuclear Reactors'(Ed. F. D'Auria), Woodhead Publishing – Elsevier, ISBN 9780081006627

D'Auria F., 2017a, Best-Estimate Plus Uncertainty (BEPU) Approach for Accident Analysis, Invited at 1st International Conference on Nuclear Power Plants (NUPP 2017), London, UK, 6th — 8th February

D'Auria F., Glaeser H., Debrecin N., 2017, Independent Assessment for new Nuclear Reactor Safety, TopSafe Conf., Vienna, Austria, Feb. 12-16

D'Auria F., Glaeser H., Debrecin N., 2017a, BEPU and Safety Margins in Nuclear Reactor Safety, Int. Conf. on Topical Issues in Nuclear Installation Safety: Safety Demonstration of Advanced Water Cooled Nuclear Power Plants, Vienna, Austria, June 6-9

Dusic M., Dutton M., Glaeser H., Herb J., Hortal J., Mendizábal R., Pelayo F., 2014, Combining Insights from Probabilistic and Deterministic Safety Analyses in Option 4 from the IAEA Specific Safety Guide SSG-2, J. Nuclear Technology, 188

EC-EURATOM, 2013, ASAMPSA2 Best Practices Guidelines for L2 PSA Development and Application, Volume 2 - Best practices for the Gen II PWR, Gen II BWR. Extension to Gen III reactors; Technical report ASAMPSA2/WP2-3/D3.3/2013-35, Brussels (B)

Glaeser H., 2017, Verification and Validation of system thermal-Hydraulic computer codes, scaling and uncertainty evaluation of calculated code results, Chapter 13 of Book 'Thermal-hydraulics of Water Cooled Nuclear Reactors'(Ed. F. D'Auria), Woodhead Publishing – Elsevier, ISBN 9780081006627

IAEA, 2000, Safety of Nuclear Power Plants, Report NS-R-1, Vienna (A)

IAEA, 2006, Fundamental Safety Principles, Report SF-1, Vienna (A)

IAEA, 2008, Best Estimate Safety Analysis for Nuclear Power Plants: Uncertainty Evaluation, Safety Report Series, SRS No 52, Vienna (A), 2008

IAEA, 2009, Safety Assessment for Facilities and Activities, Report GSR Part 4, Vienna (A)

IAEA, 2010, Deterministic Safety Analysis for Nuclear Power Plants, IAEA SSG-2, Vienna, (A)

IAEA, 2015, Consultancy at IAEA dealing with Safety Margins, Unpublished material

Jafari J., D'Auria F., Kazeminejad H., Davilu H., 2003, Reliability evaluation of a natural circulation system, J. Nuclear Engineering & Design, Vol 224, pages 79-104

Menzel F., Sabundjan G., D'Auria F., Madeira A., 2015, Using of BEPU Methodology in a Final Safety Analysis Report, Int. Conf. INAC-ENFIR, Sao Paulo (Br), Oct. 5-9

Menzel F., Sabundjan G., D'Auria F., Madeira A., 2016, Proposal for systematic application of BEPU in the licensing process of nuclear power plants, Int. J. Nuclear Energy Science and Technology, Vol. 10, No. 4, 323-337

Moretti F., Terzuoli F., D'Auria F., Mazzantini O., 2016, Instrumenting Full scale Boron Injection Test Facility to support Atucha-2 NPP licensing, Specialists Workshop on Advanced Instrumentation and Measurement Techniques for Nuclear Reactor Thermal Hydraulics SWINTH-2016, Livorno (I), June 15-17

OECD/NEA, 2004, Neutronics/Thermal-hydraulics Coupling in LWR Technology, (Vols. I, II and III), Report No 4452, ISBN 92-64-02083-7, Paris (F)

OECD/NEA/CSNI, 2017, Scaling State of the art Report – the S-SOAR, NEA/CSNI/R(2016)14, Paris (F)

Zimmermann M.A., 2011, Safety Margin Assessment (SM2A): Stimulation for further development of BEPU approaches, OECD/NEA/CSNI Workshop on Best Estimate Methods and Uncertainty Evaluations, Barcelona (Sp), November