A 'NEW' VISION FOR NUCLEAR REACTOR SAFETY

F. D'Auria (University of Pisa, Italy), H. Glaeser (retired from GRS, Germany), M. Kim (IAEA, Austria)

Abstract

The paper deals with Nuclear Reactor Safety Technology (NRST) involving fission and water cooled or moderated reactors. NRST is established since several decades, starting from the discovery of nuclear fission. Well known events, the latest one being Fukushima, have challenged the future of nuclear technology and undermined the trust of the public, of the decision makers and even of the scientific community toward nuclear safety. Innovative ideas and proposals are possibly needed to restore the confidence and escape the irreversible loss of competence which also feeds the further degradation of the sustainability for this technology.

A two-tier interconnected idea is outlined in the paper. On the one hand independent-mandatory safety analysis planned and performed according to the latest available developments in science and technology. On the other hand, feedback of analysis upon the design, construction and operation of any Nuclear Power Plant in terms of systems and related control: to this aim, characterization and continuous monitoring of expanded Safety Margins is established.

The role of safety analysis as a key part of NRST is discussed first and the innovation connected with the words 'independent' and '(systematic) Best Estimate Plus Uncertainty' is presented. The concept of continuously monitored extended safety margins is outlined in the second part of the paper.

1. INTRODUCTION

The Fukushima tragedy in 2011 might have placed a non-return clause for phasing out of nuclear fission technology producing a high amount of electricity. Actually, the flourishing period for the exploitation of the split atomic nucleus power terminated already at the time of the Three Mile Island event in 1979. Before that event, the argument of nuclear designers to the question concerning the consequences of losing the control of core cooling was denying the possibility of core melt or even of significant degradation. This was true notwithstanding the alerting results of early probabilistic studies where values greater than 10^{-4}, i.e. (roughly) one accident every 25 years for a fleet of 400 reactors, were found for the probability of severe plant damage.

The devastating and, at the same time, foreseeable accidents of TMI-2, Chernobyl-4 and Fukushima-1-3 are associated respectively loss of lifes and people loosing their living areas, with the billion $ lost for the Owner, and the trillion $ lost for the Country. A further disaster is constituted by undue delays in the operation start and exaggerated cost increases for some plants including the unit nowadays in construction in Finland. Under those circumstances any Government may put question marks to the development of nuclear programs and minimize or cancel the related benefits.

Efforts have been completed by the technological community following each of the disasters and ended-up in reinforcements of the Engineered Safety Features (ESF) and of Safety Barriers. Recently, features and capabilities like Core Catcher, Vessel Cooling, Hydrogen Recombiners and, more noticeably, Containment

Venting have been introduced or are being studied. Proposals for remote Rescue Teams have also been formulated.

All those efforts or proposals reveal not sufficient for continuing the nuclear adventure and are vulnerable in relation to the following statement: “The complex of safety measures was acceptable until the disaster and proved to be inadequate afterwards: any new complex of safety measures may suffer of the same limitation”.

The issue here is to restore the trust in the international scientific community. Therefore, core melt cannot occur and, at the same time, residual risk must be accepted; the residual risk shall be connected with an impact of a meteorite on a NPP.

In order to restore the trust, innovative approaches toward the Nuclear Reactor Safety are envisaged as necessary here. Two key targets are pursued and consist in establishing:

A) Acceptable Independent Safety Analysis.
B) Expanded Safety Margins Evaluation and Continuous Monitoring.

The purpose of the present paper is to provide the background and the framework for the proposed approaches.

2. THE PICTURE FOR NUCLEAR REACTOR SAFETY

The Nuclear Reactor Safety Technology may be perceived as entailing two main parts, the Fundamentals and the Application. This is illustrated by the sketch in Fig. 1, see also refs. [1], [2] and [3].

The Fundamentals 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 performed for the design, the licensing, the construction, the displacement, the operation and the decommissioning of any nuclear installation involving the presence of radioactive material.

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

The NRST implies the existence of a road map based on the established safety objective and becoming concrete with the design, construction and operation (including the plant dismantling and the fuel cycle) of NPPs. Acceptable safety and/or design margins shall be demonstrated for each step of the process in compliance with the safety Fundamentals. The safety and/or design margins imply the existence of acceptance criteria which are established and controlled by devoted institutions, typically Regulatory Authority. Furthermore, principles like Fail-to-Safe and As-Low-As-Reasonably-Achievable (ALARA) are part of the overall picture.

The accomplishment of safety fundamentals in the NPP design is achievable by suitable safety analysis and assessment. 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 safety margins exist.

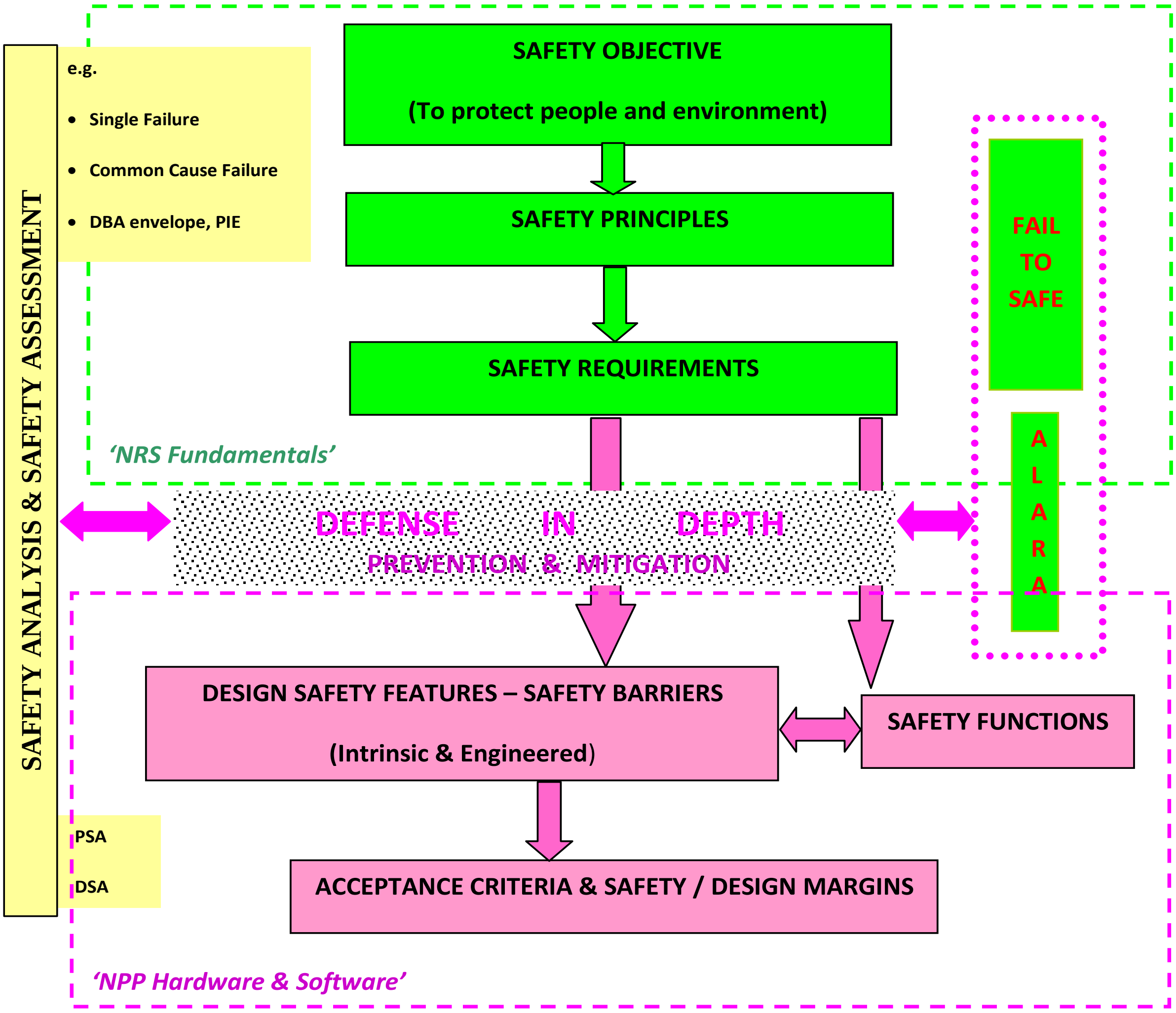

Fig. 1 – Simplified sketch for Nuclear Reactor Safety Technology.

Here, it appears worthwhile distinguishing between analysis and assessment: the first term relates to activities of designers, vendors or utilities to implement the Fundamentals into the NPP (Hardware and Software), the latter relates to confirmation typically performed under the responsibility of Regulatory Authority. Tools and procedures can be similar or even the same for analysis and assessment, however specialist groups performing the activity shall be independent upon each other.

Probabilistic Safety Analysis (or Assessment), PSA, and Deterministic Safety Analysis (or Assessment), DSA, constitute established categories within NRST. Assumptions, concepts and procedures like single-failure, Design Basis Accident, DBA, and DBA-envelope, event-tree, fault-tree or uncertainty-evaluation are part of either PSA or DSA or both.

A path is established in Fig. 1 between the safety objective (top of the sketch) and the safety margins (bottom of the sketch). The safety functions are ensuring the integrity of the design-safety features and of the safety barriers. Parameters characterizing the pink blocks of the NPP Hardware & Software are object of calculations performed within the DSA and PSA. The concepts of Prevention and Mitigation are relevant to the overall road map and shall be considered as key elements for the DiD.

A comprehensive description of individual elements of the diagram is beyond the purpose of the paper. However, some insights are given below, in relation to the roles of PSA and DSA and to the diagram-cross-cutting-issue constituted by licensing.

2.1 Role of PSA and DSA

The terms Deterministic Safety Assessment, DSA, ref. [4], are associated with the availability of qualified Best-Estimate (BE) computational tools or codes, and it is in use since the 90s. However, conservative DSA constitutes key practice for the design and the safety confirmation of existing reactors, i.e. activities performed since 50s. On the other hand, uncertainty is the key-word for the application of Best Estimate codes.

The terms Probabilistic Safety Assessment, PSA, ref. [5], are in use within the NRST since the issue of the WASH-700 (subsequently WASH-1400) by N. Rasmussen in the early 70s. Three PSA levels are distinguished to estimate the risk; those levels cover the probability and the consequences (i.e. the radiological impact) of faulting events at any time of the NPP life. Noticeably, the calculation of consequences can only be performed by DSA computational tools.

Both DSA and PSA are needed for a consistent Safety Analysis Report (i.e. primarily, chapters 15 “Accident Analysis” and 19 “Severe Accidents” of the generally accepted FSAR structure). Furthermore, a variety of interactions are envisaged and do exists between the two NRST categories.

2.2 Licensing and FSAR

The NRST activities which are supervised and imposed by a Regulatory authority constitute the licensing process. The process follows specification and rules which are part of the laws of the Country where the NPP is supposed to operate or where it is designed.

The FSAR is the compendium of information concerned with the safety of the specific NPP and includes the demonstration of acceptability of the NPP. The Safety Analysis is part of the licensing process and is documented in the FSAR.

The current structures of the licensing process and of the FSAR constitute a reference for the proposal hereafter. This is specifically true for the acceptance criteria which are only responsibility of the Regulatory Authority in charge. Rather, the procedures and the approaches as well as the analytical techniques and the ‘amount and the modalities of application’ of computational tools are concerned by the proposal.

3. THE SAFETY ANALYSIS AND BEPU

3.1 Final Safety Analysis Report

Three types of (safety) analysis, at least, can be distinguished, making reference to the prediction of accident scenarios in NPP:

- Quick analysis, i.e. performed without qualification bases.
- Reasonable analysis, i.e. performed by qualified analytical tools without procedures or repeatability test.

- Acceptable analysis, i.e. based on quality procedures, acceptance criteria and ensuring traceability and reproducibility of results.

The resources needed to perform the analysis of an assigned NPP transient are indicated by X, 10X and 100X in relation to the classified bullet items. The quantity X shall be interpreted as an order of magnitude andmay correspond to 10^4 $ or 2 man-weeks.

Here, the attention is focused only to the third bullet. Furthermore, it is assumed that the analysis is performed by NRST specialists which are independent of the Designer or the Owner of the NPP. Therefore, key words here are FSAR (section 2.2, additional details in section 3.1) and the analysis approach called Best Estimate Plus Uncertainty (BEPU).

The ALARA principle already introduced as a cross-connecting path between principles and application of NRST (Fig. 1) shall be taken at the basis of BEPU: the words *as Low as Reasonably Achievable* shall be translated into *as Accurate as Reasonably Achievable* in the case of BEPU.

BEPU involves the use of the most recent analytical techniques, the recognition of Validation for the computational tools and, following-on, the characterization of expected errors or the evaluation of uncertainty of the computed results. BEPU also corresponds to what is called 'option 3' for performing deterministic safety analysis as given in ref. [4].

Assembling the top level competence in relation to each of the listed topics, on the one hand is an obligation to demonstrate the safety of any nuclear installation, on the other hand is difficult to achieve and to preserve even by established NPP design companies. A proposal for a suitable Consortium of Competences can be found in ref. [6].

3.2 Innovation for Safety Analysis

The first key innovation is that the Safety analysis shall be carried out by expert technologists independent of the Owner, of the Vendor or the Designer for the concerned NPP.

The second key innovation is that the latest qualified analysis techniques shall be adopted as well as the latest qualified findings from research.

The third key innovation is the objective of homogeneity in the NRST matters: analyses including calculation processes shall not be limited to the accident analysis, but encompass whatever topic connected with the design, the construction and the operation of the NPP.

The fourth key innovation, subject for the following chapter, consists in creating a technological connection (systems and/or controls) between safety analysis and the hardware of the NPP.

The first innovation is challenged by the unsurmountable issue of the proprietary data and information: NPP Designer and Owners do not share data, even though Regulatory Authorities impose mandatory requirements for the availability of data. Thus, owing to reasons directly connected (but not only) with intellectual properties, analytical capabilities and market competition, NPP sensible data remain unavailable to the screening of experts independent from the NPP Designer or Owner. A proposal to handle sensitive proprietary data by 'independent' experts without creating damage to the ownership of those data is formulated in ref. [6].

Only a few Regulatory Authority bodies exist which have the capability to invest in research and may follow the myriad developments in each of the NRST sectors: this poses a difficulty for the second innovation. Furthermore, the Industry may have the same limitation and no interest in proposing innovation without demand. Then, a lag of 10-30 years establishes between applicable (qualified) research findings and application. This is frustrating for the specialists in the various sectors and undue for the safety: this situation can be observed as one reason of the three major nuclear tragedies.

Third innovation: Owing to historical reasons, accident analysis received suitable attention by NRST actors. However, accidents, i.e. not only the three major tragedies, happened either in peripheral areas or following precursory events which brought the NPP in conditions outside those considered for accident analysis. Therefore, homogenization of NRST topics is needed as far as related analysis are concerned and, at the same time a connection between DSA and PSA should be strengthened.

So far the strategic objective of safety analysis is to demonstrate the acceptability of the NPP against assigned criteria. Here, the fourth innovation, it is proposed that 'each' outcome of safety analysis becomes a target for a physical measurement or a signal from the NPP status which shall be continuously monitored. A suitable hardware shall allow the monitoring of the sum of safety margins. For instance, in the case of TMI-2 leaking pressurizer valve, presence of a manual valve in the auxiliary feed-water line having the possibility to remain close, etc. shall prevent the operation of any reactor unit well before conditions are created for the occurrence of a safety relevant event.

4. THE SAFETY MARGINS

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 Power Plants operate safely in all modes of operation 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, material condition), to containment (pressure, 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 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. In addition, the concepts of safety margins and of quantifying changes in safety margins are appearing 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 concept of 'Safety Margin' (directly extended here to the concept of Design Margins) is consistent with the NRST framework depicted in Fig. 1 and can be directly characterized from Fig. 2. The concepts 'Safety Limits' and 'Licensing Margins' are also relevant here.

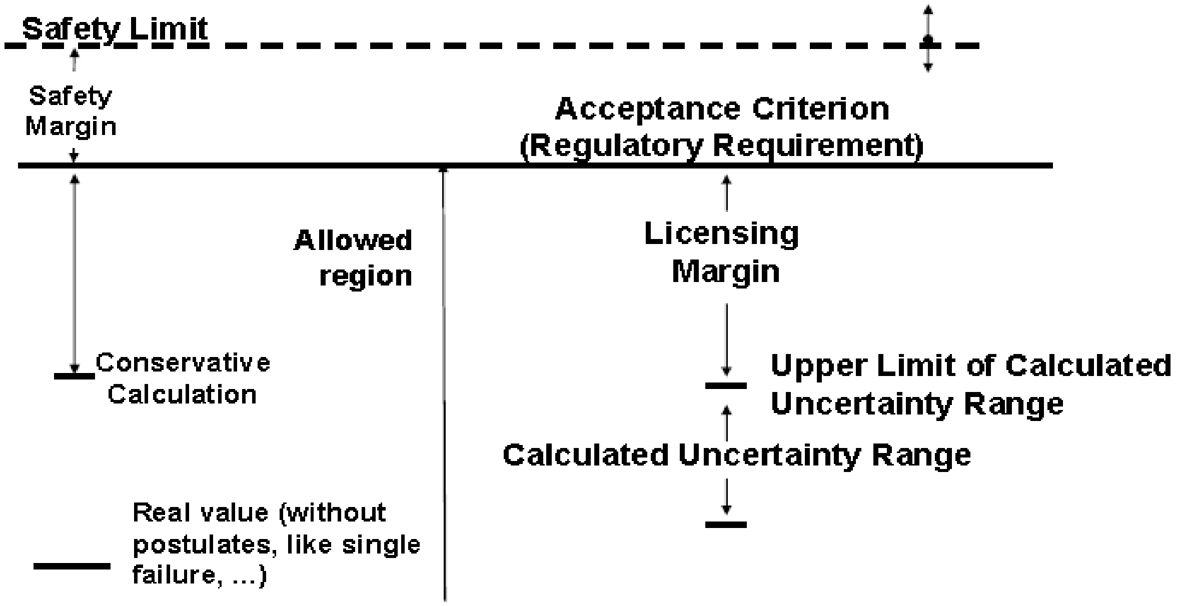
Safety Limit
Safety Margin
Acceptance Criterion
(Regulatory Requirement)
Allowed region
Licensing Margin
Conservative Calculation
Upper Limit of Calculated Uncertainty Range
Calculated Uncertainty Range
Real value (without postulates, like single failure, ...)

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

In the following, the words Safety Margins (SM) have a broader meaning and are used in combination with the words Design Margin (DM). The concepts of SM (and DM) are expected to be introduced in relation to the following aspects (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'.

4.1 The multi-dimensional space to evaluate Safety Margins

It becomes clear that the definition of Safety Margins and Design Margins 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 according to ref. [7]. The key dimensions for the space embracing the definition of SM can be defined as:

A) The key elements characterizing NRST.

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 A1) to A6), B1) to B5), C1) to C19) and D1) to D7) are defined 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 safety analysis discussed in Chapter 3.

A6) DSA Elements, i.e. DE-1 to DE-m, i.e. according to results of safety analysis discussed in Chapter 3.

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) 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 NRST and NPP technologies.

4.2 The procedure for the application of the SM Matrix

Based on the definitions outlined in the previous section, 35 (thirty-five) SM tables are created which constitute the multidimensional SM Matrix, ref. [7].

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 Safety Margins definition related to non-dimensional Acceptance Criteria set at the unity value. In relation to each Safety Barrier and to each Safety Function, ‘n’ SM can be defined. One average SM can be defined per each Safety Barrier and each Safety Function. One average SM can be combined and estimated as a function of time per each NPP, specifically following any modification or any (relevant) operational event.

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.

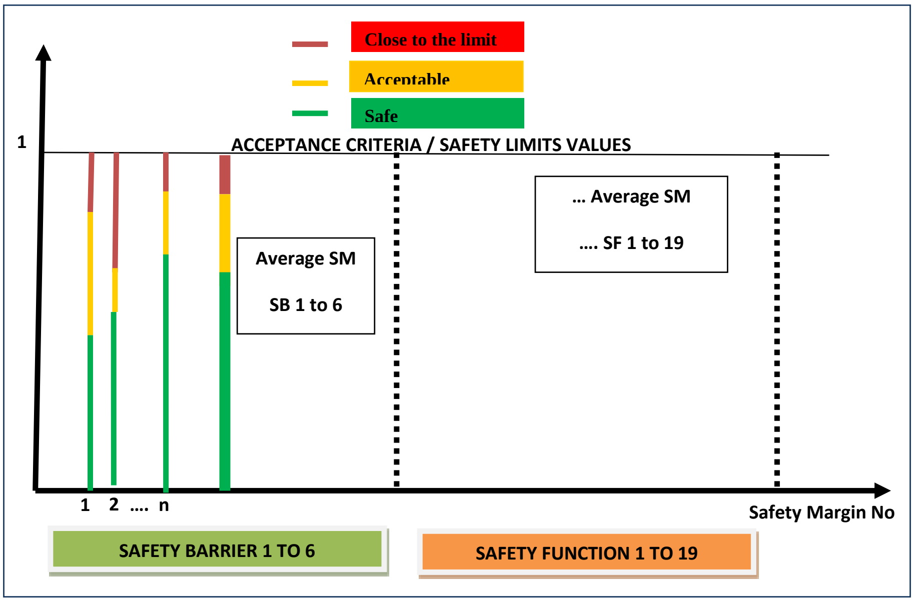

Fig. 3 – Application of the Safety Margin Matrix.

4.3 Innovation for Safety Margins

The extensions of the concept of Safety Margins constitutes the first proposed innovation. SM shall be systematically derived in relation to each NRST topic.

The second innovation is the continuous monitoring of SM. This implies specific systems and related controls installed in each NPP. Such a system would have created a 'red-alarm' for each of the three nuclear tragedies well before the actual start of the accident.

The third innovation is a better connection between highly qualified deterministic and probabilistic safety analysis.

The fourth innovation is the tight connection between safety analysis and safety margin: whatever is the topic of safety analysis, a suitable hardware shall allow the monitoring of the sum of safety margins. For instance, the combination of a certain number of signals (e.g. in the case of TMI-2 leaking pressurizer valve, presence of a manual valve in the auxiliary feed-water line having the possibility to remain close, etc.) shall prevent the operation of any reactor unit well before conditions are created for the occurrence of a safety relevant event.

5. CONCLUSIONS

An ambitious proposal is outlined in the paper which is motivated by the apparently irreversible decline of the nuclear technology based upon water cooled reactors. The complexity of nuclear technology is also reflected in the paper and may be seen as a further motivation for the proposal: ironically, the complexity of the NRST brings to expertise build-up periods as long as 30 years which is close to the working life: once an expert has acquired good knowledge and experience he/ she is ready for retirement. Finally, the severe accidents experienced by the nuclear industry, Three Mile Island in 1979, Chernobyl in 1986 and, primarily, Fukushima in 2011 somewhat drove the present proposal. Key topics in nuclear safety technology constitute the objective of the proposal, but not all related aspects are considered: noticeably, human factors and systematic lessons learned from operational and accident experiences are not discussed.

The two-tier proposal can be summarized as the introduction of the BEPU based independent safety analysis and the definition and proposed exploitation of a multidimensional Safety Margins Matrix. The following achievements are expected:

- ⇨ An innovative additional safety barrier is created based on analysis-systems-monitoring.
- ⇨ Core degradation, better substantial and uncontrolled radiological impact on the environment and 'nuclear' casualties should become again (as was the case before TMI-2) 'impossible or part of the residual risk'.
- ⇨ There is no defense against large radiological release if a meteorite hits the NPP: the probability of this event shall be evaluated and the occurrence itself monitored before it happens. The probability of that event multiplied by the consequences shall also be used to bound the risk associated with any concerned NPP.
- ⇨ Residual risk should be quantified as from before and eventually accepted by the scientific community, the decision makers and the population.

References

[1] IAEA, 2006, Fundamental Safety Principles, Safety Fundamentals No. SF-1, Vienna (A)

[2] IAEA, 2000, Safety of Nuclear Power Plants: Design, Requirements No. NS-R-1, Vienna (A)

[3] IAEA, 2009, Safety Assessment for Facilities and Activities, General Safety Requirements No. GSR Part 4, Vienna (A)

[4] IAEA, 2009, Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide No. SSG-2, Vienna (A)

[5] IAEA, 2010, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide No. SSG-4, Vienna (A)

[6] D'Auria F., Debrecin N., 2014, Perspectives in Licensing and Nuclear Reactor Safety Technology, Third International Scientific and Technical Conference "Innovative Designs and Technologies of Nuclear Power" (ISTC NIKIET-2014), Moscow, Russia, October 7-10, 2014

[7] IAEA, draft to be issued, Concepts for Safety and Design Margins of NPP, Report TECDOC