NARSIS

New Approach to Reactor Safety ImprovmentS

WP3: Integration and Safety Analysis

Del 3.8 – Development and Description of E-BEPU Method – Part A “theoretical basis” – Part B “practical application” will be presented in Del 4.5

Del 3.9 – Use of E-BEPU for Evaluation of Defence-in-Depth

This project has received funding from the Euratom research and training programme 2014-2018 under Grant Agreement No. 755439.

Project Acronym:	NARSIS		
Project Title:	New Approach to Reactor Safety Improvements		
Deliverable:			
Month due:	D3.8 – M36	**Month delivered:**	M24
	D3.9 – M24		M24
Leading Partner:	NUCCON		
Version:	V1		

Primary Authors: Milorad Dusic, Javier Hortal, Rafael Mendizabal, Fernando Pelayo

Other contributors:

Deliverable Review:

- **Reviewer #1:** Ivica Basis, Ivan Vrbanic - APPoS **Date:** 08/2019
- **Reviewer #2:** Alberto Ghione, Lucia Sargentini - CEA **Date:** 09/2019

Reviewer #3: Piotr Mazgaj, Piotr Darnowski – WUT **Date:** 09/2019

Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of contents

List of Figures

List of Tables

List of Abbreviations

ANS	American nuclear society
ANSI	American national standards institute
AOO	anticipate operational occurrences
BE	best estimate
BEMUSE	best estimate methods – uncertainty and sensitivity evaluation
BEPU	best estimate plus uncertainty
BIC	boundary and initial conditions
CDF	core damage frequency
CDF	cumulative distribution function (Chapter 4)
CFR	code of federal regulation
CNS	convention on nuclear safety
CSAU	code scaling, applicability and uncertainty evaluation methodology
CSNI	committee on the safety of nuclear installations
CSS	commission on safety standards
DBA	design basis accident
DBC	design basis condition
DBT	design basis transient
DEC	design extension condition
DEC-A	design extension condition without core melt
DEC-B	design extension condition with core melt
DiD	defence-in-depth
DNB	departure from nucleate boiling
DSA	deterministic safety analysis
E-BEPU	extended best estimate plus uncertainty analysis
ECCS	emergency core cooling system
ENS	European nuclear society
EPReSC	emergency preparedness and response standards committee
EU	European commission
EUR	European utility requirements
FCHF	fuel rod in critical heat flux condition
FOM	figure of merit
GSR	general safety requirements
IAEA	international atomic energy agency
ITL	increased tolerance level
KTA	kerntechnischer ausschuss (German safety standards)

LOCA	loss of coolant accident
LOOP	loss of offsite power
MSLB	main steam line break
NEA	nuclear energy agency
NO	normal operation
NPP	nuclear power plant
NS	nuclear safety
NSD	nuclear safety directive
NUSSC	nuclear safety standards committee
OECD	organization for economic cooperation and development
PIE	postulated initiating event
PS	plant states
PSA	probabilistic safety assessment
RAC	regulatory acceptance criteria
RASSC	radiation safety standards committee
RCS	reactor coolant system
RHWG	reactor harmonization working group (from WENRA)
SBO	station black-out
SF	safety fundamentals
SLB	steam line break
SMAP	safety margin action plan
SSG	specific safety guide
SSR	specific safety requirements
SRS	safety report series
SRS	simple random sample (chapter 4)
STL	standard tolerance level
TRANSSC	transport safety standards committee
TS	technical specifications
UMS	uncertainty method study
UPV	polytechnic university of valencia
US NRC	united states nuclear regulatory commission
VDNS	Vienna declaration on nuclear safety
WASSC	waste safety standards committee
WENRA	west European nuclear regulators' association

Executive Summary

Safety analysis of nuclear power plants and, to some extent, of other nuclear facilities has been historically developed at two levels. In the first level the objective is to ensure that the plant design verifies the safety design specifications, with the focus on safety systems which provide protection and/or mitigation against abnormal occurrences in different operational states. In the second level, the objective is to estimate the potential for plant states that exceed the design provisions and may result in consequences beyond the design limits. Typically, the first level analysis has been based on deterministic methodologies while the second level has relied on the use of probabilistic methodologies.

For some time, practitioners of safety analyses for nuclear power plants have been making efforts to combine deterministic and probabilistic safety analysis methods in order to achieve coherent methodologies that would take the advantages of both approaches when assessing any aspect of the safety of nuclear installations. In many cases these efforts resulted in essentially deterministic safety analysis (DSA) taking insights/results from the probabilistic safety analysis (PSA) where needed or vice versa.

In the second level of safety analysis, some recent developments have gone further and the resulting methodologies, particularly those grouped under the denomination of “dynamic PSA”, have reached the point of being considered combined deterministic-probabilistic methodologies, although they are still considered as experimental and have been applied only to a very limited extent.

In the field of the first level analysis, however, there has been much less developmental activity and the Extended Best Estimate plus Uncertainty Analysis (E-BEPU) is probably one of the first attempts to show how both, deterministic and probabilistic methods can be combined to bring a truly integrated method for safety assessment of the design of nuclear installations. This study presents in some detail the approach to be taken in applying the E-BEPU methodology. The differences to the existing, conventional methodologies are described in this study as well as all the advantages that the combined E-BEPU can bring when assessing the safety design of nuclear installations, including better determination of safety margins, avoidance of cliff-edge effects, evaluation of defence-in-depth and application to design extension conditions.

1. Background

All international safety standards applicable to existing or new nuclear power plants (NPPs) require the use of different types of safety analysis to demonstrate the level of safety of nuclear facilities. Such level relies on systems, structures and features intended to avoid undesired effects resulting from normal or abnormal operation of the facility. Safety analysis has been typically performed at two levels. In the first level the goal is to ensure that the plant design verifies the safety design specifications, i.e., that safety systems, structures and features perform as expected under the conditions assumed as design basis. The goal of the second level is to verify that the final plant design is safe enough as to make the plant operation acceptable. Due to the importance of safety standards the next section will provide a very brief overview of the most relevant ones in the international context.

1.1 Current International Safety Standards for Nuclear Installations

1.1.1. The EU has the most advanced legally binding and enforceable framework for nuclear safety which is of utmost importance for the industry development and for protection of people and the environment. The Council Directive 2014/87/Euratom of 8 July 2014 [24] which brings the amendment to the Directive 2009/71/Euratom establishing a Community framework for the nuclear safety of nuclear installations (commonly referred to as the amended Nuclear Safety Directive) brings these standards to even a higher level. The original Council Directive 2009/71/Euratom imposes obligations of the Member States to establish and maintain a national framework for nuclear safety and reflects the provisions of the main international instruments in the field of nuclear safety, namely the Convention on Nuclear Safety, as well as the IAEA Safety Fundamentals. After the Fukushima Daiichi accident “stress tests” were performed community-wide but in addition, the European Council also called on the Commission to review, as appropriate, the existing legal and regulatory framework for the safety of nuclear installations and propose any improvements that may be necessary. The European Council also stressed that the highest nuclear safety standards should be implemented and continuously improved in the European Union. As a consequence, amended Nuclear Safety Directive has been prepared and entered into force in July 2014.

1.1.2 WENRA, the Western European Nuclear Regulators’ Association has issued two documents that are of high relevance to nuclear safety of NPPs:

Report on Safety Reference Levels for Existing Reactors [28] and

Report on Safety of new NPP designs [16]

The objective of the development of Safety Reference Levels was to increase harmonization within WENRA countries on safety requirements issued by the regulatory bodies and their implementation in existing NPPs. Initially they identified 18 areas where harmonization was considered as necessary. After the Fukushima Daiichi accident, an additional 19th issue has been included to cover natural hazards (extreme weather conditions, external flooding, and seismic events). Major changes after the Fukushima Daiichi accident have also been in the area of Design Extension Conditions (DEC) – Issue F, where clear differentiation between DEC without core melt (DEC A) and DEC with core melt (DEC B) has been introduced, and in addressing the DEC aspects for the spent fuel pool and multi-unit sites. NPP autonomy for a justified time has also been introduced.

The Safety Reference Levels’ emphasis is on nuclear safety, primarily focusing on safety of the reactor core and spent fuel. They specifically exclude nuclear security and, with few exceptions, radiation safety. Their latest version represents, in addition to good practices in

WENRA countries, objectives for safety improvements taking into account the lessons learned from the Fukushima Daiichi accident.

The intention of the document on Safety of new NPP design was to develop common positions on selected key safety issues and safety expectations for the design of new NPPs. The document addresses:

- WENRA safety objectives for new NPPs
- Selected key safety issues divided into 7 Positions and
- Lessons learned from the Fukushima Daiichi accident (covering 6 conclusions on issues presented in the above 7 positions).

1.1.3. IAEA, the International Atomic Energy Agency, is internationally recognized as a leader in the development of nuclear safety standards. These standards are non-binding (except for States in relation to IAEA assisted operations) but widely accepted and serve as reference for all countries, including EU Member States, to formalize their national binding and non-binding nuclear framework.

The IAEA Statute authorizes the IAEA to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for their application. With a view to ensuring the protection of people and the environment from harmful effects of ionizing radiation, the IAEA Safety Standards establish fundamental safety principles, requirements and measures to control the radiation exposure of people and the release of radioactive material to the environment, to restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation, and to mitigate the consequences of such events if they were to occur. The standards apply to facilities and activities that give rise to radiation risks, including nuclear installations, the use of radiation and radioactive sources, the transport of radioactive material, the management of radioactive waste and emergency preparedness and response. For this reason, 5 safety standards committees have been established, with the aim to prepare and review safety standards in their thematic areas, namely Nuclear Safety Standards Committee (NUSSC) for nuclear safety, Radiation Safety Standards Committee (RASSC) for radiation safety, Waste Safety Standards Committee (WASSC) for the safety of radioactive waste, Transport Safety Standards Committee (TRANSSC) for the safe transport of radioactive material and EPReSC for emergency preparedness and response. All five Committees report to the Commission on Safety Standards (CSS), which oversees the IAEA safety standards programme.

Apart from the safety standards, the IAEA is developing also the security standards. Safety measures and security measures must however be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security.

The IAEA safety standards [1-7] reflect an international consensus on what constitutes a high level of safety for protecting people and the environment from harmful effects of ionizing radiation. They are published in 3 categories, as Safety Fundamentals, Safety Requirements and Safety Guides.

The IAEA Safety Series start with the top document, SF-1 on Safety Fundamentals. The IAEA Safety Fundamentals consist of 10 safety principles. Under the Safety Fundamentals,

the IAEA Safety Requirements are produced, with the objective to set up the requirements which are necessary to fulfil 10 safety principles.

The IAEA Safety Requirements are divided into two parts; General Safety Requirements (GSR) and Specific Safety Requirements (SSR).

There are 7 General Safety Requirements; Part 1: Governmental, Legal and Regulatory Framework for Safety, Part 2: Leadership and Management for Safety, Part 3: Radiation Protection and Safety of Radioactive Sources, Part 4: Safety Assessment of Facilities and Activities, Part 5: Predisposal Management of Radioactive Waste, Part 6: Decommissioning and Termination of Activities and Part 7: Emergency Preparedness and Response.

Specific Safety Requirements comprise of 6 volumes: NS-R-3 (Rev 1): Site Evaluation for Nuclear Installations, SSR-2/1(Rev 1): Safety of Nuclear Power Plants: Design, SSR-2/2 (Rev 1): Safety of Nuclear Power Plants: Commissioning and Operation, SSR-3: Safety of Research Reactors, NS-R-5 (Rev 1): Safety of Nuclear Fuel Cycle facilities, SSR-5: Disposal of Radioactive Waste and SSR-6: Regulations for the Safe Transport of Radioactive Material. Underneath of these Safety Requirements there is an entire fleet of corresponding Safety Guides which provide guidance on how to fulfil the higher level requirements.

1.1.4. Vienna Declaration on Nuclear Safety (VDNS) [25] has been adopted following the efforts and initiatives to strengthen the review process under the Convention on Nuclear Safety (CNS). Following the efforts and initiatives that took place nationally, regionally and internationally after the Fukushima Daiichi accident, the Contracting Parties met at the Diplomatic Conference to amend the CNS in February 2015. The initiative for the amendment of CNS came from the Swiss Confederation with particular emphasis on the amendment of Article 18 of the CNS. The initiative was presented in order to bring the nuclear safety standards in other regions to the same high level as prescribed to the EU countries through the amended NSD. It would assure that high safety standards are applied worldwide and that these are not undermined by the use of cheaper or outdated technology.

The Diplomatic Conference of the Convention on Nuclear Safety at the end adopted the so-called Vienna Declaration on the 9th of February 2015. It has only 3 Articles. The first one addresses new nuclear power plants, the second one the existing nuclear power plants and the third the obligation to follow the IAEA Safety Standards.

1.1.5. The European Utility Requirements [15] started work in 1991 when major electricity producers joint effort to harmonize national efforts in the development, design and licensing of Light Water Reactor plants. The EUR organization started with 5 partners in 1991 and is comprising of 14 partners today. In the period from 1991 until today, several revisions took place, Revision A was published in 1994, Revision E in 2016. The aim of the European Utility Requirements is to promote harmonization of requirements for Generation III NPPs across Europe (and worldwide). Generation III NPPs are considered to be an evolution from the Generation II NPPs characterized by:

- improvements in nuclear safety with additional redundancy and diversity and inclusion of passive systems,
- having standardized design that would reduce the licensing time,
- higher availability and operational life of typically 60 years,
- increased fuel and thermal efficiency and
- more robust design.

The aim was to harmonize the requirements to which Light Water Reactor NPP to be built in Europe will be designed, built, commissioned, operated and maintained. In addition to

harmonization it will bring also the economic benefits by reducing costs in design, commissioning and operation, the EUR requirements require NPPs to be designed in a way to have low impact on the environment and population by minimizing radioactive and chemical releases.

1.2. Safety analysis in the international safety standards

All the above described international safety standards have a common goal of enhancing the safety of existing and new NPPs. All of them base their judgement on the level of nuclear safety on different kinds of safety analysis which in a broad sense can be divided into deterministic and probabilistic safety analysis. All of the above international safety standards explicitly call for both types of the analysis to be used in the safety assessment process.

In 2009 the International Atomic Energy Agency (IAEA) published in its Safety Standards Series the Specific Safety Guide SSG-2 on Deterministic Safety Analysis for Nuclear Power Plants [1]. It is the first IAEA document in their Safety Standards Series that deals with deterministic safety analysis. It is largely based on an earlier IAEA publication in the Safety Report Series, namely SRS # 23 on Accident Analysis for Nuclear Power Plants [2]. The difference however in presenting the methodology for the performance of deterministic safety analysis in Safety Standards Series (SSG-2) or in Safety Report Series (SRS#23) lies in the fact that SSG-2 was published with the consensus of all IAEA Member States, which is not the case for SRS#23.

Fig. 1.1 presents the logical flow which led to the publication of SSG-2 and the demand for the development of methodology to be applied when performing deterministic safety analysis (DSA).

The top safety document in the IAEA Safety Standards Series is Safety Fundamentals, SF-1[3]. It consists of ten fundamental safety principles which need to be fulfilled in order to assure nuclear safety. The ten fundamental safety principles constitute the basis on which to establish safety requirements for protection against exposure to ionizing radiation under the

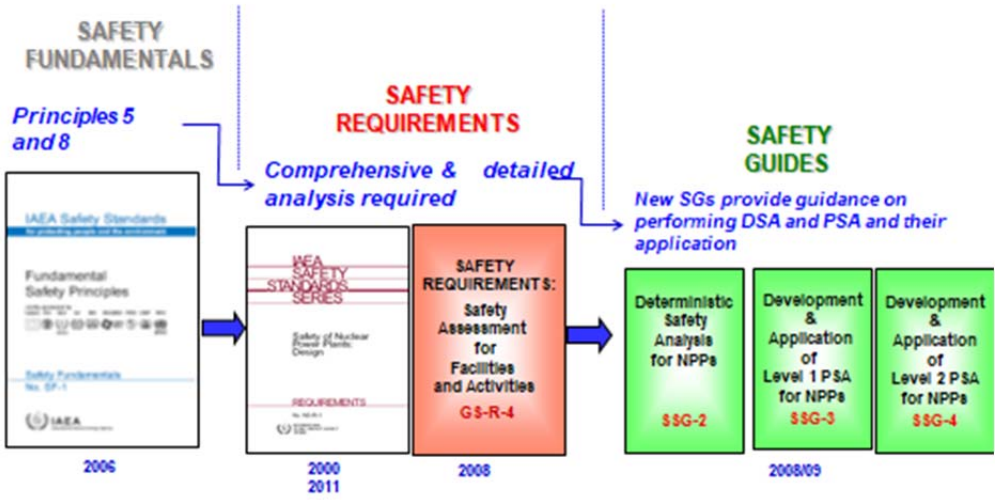

Figure 1.1: Safety Assessment in the IAEA Safety Standards

IAEA's safety standards programme and provide the rationale for its wider safety related programme. Even though, the totality of safety measures taken to ensure the protection of

human life and health and the environment against exposure to ionizing radiation is detailed and technically complex, the ten fundamental safety principles are written in a common language but in a way to encompass the entire spectrum of actions needed. Principle 5 calls for the optimization of protection and states that “protection must be optimized to provide the highest level of safety that can reasonably be achieved”. It gives basis for the utilization of probabilistic safety analysis. Principle 8 calls for prevention of accidents and states that “all practical efforts must be made to prevent and mitigate nuclear or radiological accidents”. As such, it provides basis for the utilization of DSA.

The next level of the IAEA Safety Standards Series is Safety Requirements which set the requirements that must be fulfilled in order to assure that ten safety principles are achieved. To achieve principles 5 and 8 the safety requirements call for a comprehensive and detailed safety analysis to be performed. This is written in several IAEA Safety Requirements but most notably in the Safety Requirement on Design of Nuclear Power Plants – SSR 2/1 [4] and Safety Requirement on Safety Assessment for Facilities and Activities – GSR Part 4 [5]. In these two documents it is stated that both deterministic and probabilistic method shall be utilized when assessing the safety of nuclear installations.

The next level in the IAEA Safety Standards Series is Safety Guides which provide guidance on how to fulfil the necessary requirements. Therefore, the IAEA developed two guidance documents on Development and Application of Probabilistic Safety Analysis for Nuclear Power Plants; SSG-3 for Level 1 [6] and SSG-4 for Level 2 [7]. The third guidance document is SSG-2 that provides guidance for the performance of DSA for Nuclear Power Plants.

SSG-2 provides recommendations and guidance on the use of DSA and its application to nuclear power plants. It is written in compliance with the IAEA Safety Requirements publications on Safety of Nuclear Power Plants: Design and Safety Assessment for Facilities and Activities. DSA are to be applied when analyzing anticipated operational occurrences (AOO), design basis accidents (DBA) and design extension conditions (DEC). As will be described in the next section, several options exist for the performance of DSA, depending on initiating events and transients to be analyzed as well as on the information that is required as the result of the analysis. DSA is the only method, which can reveal the remaining safety margins after an incident or a transient.

1.3. Four options for the performance of deterministic safety analysis in SSG-2

In SSG-2 four options are presented as possibilities for the performance of deterministic safety analysis. These options are summarized in Table 1.1 below.

Applied codes	Input & BIC (boundary and initial conditions)	Assumptions on systems availability	Approach	Regulation
Conservative codes	Conservative input	Conservative assumptions	Deterministic*	10 CFR § 50.46 Appendix K
Best estimate (realistic) codes	Conservative input	Conservative assumptions	Deterministic	SG NS-G-1.2 para 4.89
Best estimate (realistic) codes	Conservative input + uncertainty	Conservative assumptions	Deterministic	SG NS-G-1.2 para 4.90
Best estimate (realistic) codes	Realistic input + uncertainty	PSA-based assumptions	Deterministic + probabilistic	Risk informed

Table 1.1: Four Options from the IAEA Safety Guide SSG-2

It should be noted that the IAEA SG NS-G-1.2 has been superseded by the IAEA GSR Part 4 and the IAEA SSG-2 but they have been retained in the last column of the Table 1.1 as it was for the first time where BE and BEPU have been introduced. Similarly, the new revision of SSG-2 Rev 1 (2019) does not include E-BEPU as option 4 and therefore the old version of SSG-2 has been used as reference for this work.

The first option is a rigorous conservative option where conservative codes and models are used as well as conservative assumptions on initial and boundary conditions for the evaluation of AOOs and DBAs. This approach has been established already in 1974 when the United States Nuclear Regulatory Commission (US NRC) published 10 CFR 50.46 [8] establishing the acceptance criteria for the emergency core cooling systems for light water reactors, addressing safety limits that must be assured under loss of coolant accident (LOCA) conditions. These are:

- Maximum zircaloy cladding temperature,
- Maximum local oxidation of cladding,
- Maximum amount of hydrogen generated by chemical reaction of the zircaloy cladding with water and/or steam,
- Coolable core geometry,
- Long term cooling

Additionally, this former US regulation, being prescriptive, requires that the evaluation models to be used in licensing safety analysis must follow the conservative approach established in Appendix K to 10 CFR 50. This option was the unique one for 15 years. In the meantime extensive experimental methods were conducted in order to better understand the thermal-hydraulic phenomena. In addition, the computer capacities largely increased and all this led to adopting a more performance oriented regulatory approach, keeping the same five above mentioned criteria, but offering the possibility of adopting a best estimate approach for the evaluation models.

This development led to the second option as described in SSG-2. While using the more realistic and less conservative models, the analysts are required to keep the conservative input for initial and boundary conditions. The US NRC published in 1989 (reviewed in 2013) the Regulatory Guide 1.157 entitled Best-Estimate Calculations of Emergency Core Cooling System Performance [9]. At the same time, the IAEA Safety Guide NS-G-1.2 on Safety Assessment and Verification for Nuclear Power Plants (which later on became superseded by SSG-2) in its paragraph 4.89 states that:

> *"The computer code model parameters, initial conditions and equipment availability assumptions that underlie their use have traditionally been highly conservative with bounding, conservative values used for all analysis parameters. However, in the past this has sometimes led to misleading sequences of events, unrealistic time-scales being predicted, and some physical phenomena being missed. Bearing in mind these shortcomings and the current maturity of best estimate codes, they should be used in a safety analysis in combination with a reasonably conservative selection of input data and a sufficient evaluation of the uncertainties of the result."*

The third option in SSG-2 has its roots in the 1989 revision of the aforementioned "ECCS rule" (10 CFR 50.46), which opened the doors to the use, in LOCA/ECCS analysis, of methodologies based on realistic (best estimate) models/codes and supplemented with uncertainty analyses of their results (BEPU methodologies). The rule allowed the user to choose between the already existing conservative approach (based on Appendix K) and the BEPU approach. Furthermore, the revised rule required a probabilistic modelling of the uncertainty. The two choices differ in how the regulatory acceptance criteria (RAC) must be

satisfied: for the conservative approach, the fulfilment must be strict, while the BEPU approach requires a fulfilment “with high probability”.

After the release of the amended ECCS Rule, the USNRC published the NUREG/CR-5249 (“Quantifying Reactor Safety Margins”), presenting the CSAU (“Code Scaling, Applicability and Uncertainty Evaluation Methodology”), which can quite rightly be regarded as the first systematic BEPU methodology.

The already mentioned IAEA Safety Guide NS-G-1.2 in paragraph 4.90 introduces the BEPU Option as follows:

> *“It may also be acceptable to use a combination of a best estimate computer code and realistic assumptions on initial and boundary conditions. Such an approach should be based on statistically combined uncertainties for plant conditions and code models to establish, with a specified high probability, that the calculated results do not exceed the acceptance criteria.”*

All the above three options have been utilized for AOOs and DBAs already for more than 20 years [10]. For DEC however, when determining what measures should be taken to mitigate the consequences, uncertainty analysis is usually not performed due to large variations. The reasons for moving from the purely conservative option to options 2 and 3 have been indicated already in the IAEA Safety Guide NS-G-1.2 and can be summarized as follows:

- The use of conservative assumptions may sometimes lead to incorrect predictions on the development of an event or might indicate wrong timescales. In addition it may also not capture some important physical phenomena. All this may lead to the omission or incorrect representation of some important sequences that constitute the accident scenario.

- In almost all cases when conservative approach is taken, the apparent safety margins are much smaller than those present in reality. If properly assessed such safety margins can be usefully utilized to improve operational flexibility.

- Options 2 and 3 better represent the important physical behavior of the plant and as such also better or at least more realistic comparison with the acceptance criteria.

Option 2 (Best Estimate – BE) and especially option 3 (Best Estimate with Evaluation of Uncertainties – BEPU) are obviously more demanding in computational terms. Therefore, in cases where large safety margins exist, it might be sufficient to apply a single conservative calculation rather than performing a number of calculations which are necessary for the evaluation of uncertainties required by option 3.

However, where safety margins are expected to be smaller, it is worthwhile to invest more computational efforts and perform best-estimate calculation with evaluation of uncertainties to avoid pitfalls mentioned above in using purely conservative approach. In addition, a more precise evaluation of actual safety margins relating to the limits and set points provide the opportunity for the introduction of additional operational flexibility and reducing the number of unnecessary reactor scrams or actuations of the protection systems. This is of particular importance when assessing the impact of plant modifications or for the assessment of plant life extension. In all such cases, the compliance with the regulatory acceptance criteria under the new conditions has to be demonstrated and usually such plant modifications erode the existing safety margins and therefore more precise identification of the available safety margins is necessary which can best be achieved by using BEPU analysis. The fact is that moving from conservative to the best-estimate approach, the calculations show larger margin from the calculated results to the RAC. In moving to option 3, this difference/margin is usually

bigger even if we compare the upper bound of the results with uncertainties with the results of a single calculation using options 1 or 2.

Option 3 i.e. BEPU includes a detailed evaluation of uncertainties. In performing safety analysis one compares the calculated results with the RAC. These acceptance criteria are set by the regulatory body as a value where certain barrier will remain intact. The failure of the barrier is not an exact value (due to our limited knowledge of the precise physical phenomena involved), so that it is described by a probability distribution. The regulatory acceptance limit is a low (or very low) quantile of this probability distribution.

On the other hand, the calculation results when modelling an accident or a transient is also an uncertain magnitude, due to uncertainties in the model as well as in initial and boundary conditions. Thus, the results are described through probability distributions, and the values to be compared with the acceptance limits are typically chosen as tolerance limits 95/95, meaning that they are 95% confidence limits of the 95th quantile of the distribution. The pair formed by the confidence level and the quantile order is termed “tolerance level”. The value 95/95 will be termed “Standard Tolerance Level – STL” throughout the present study.

In the last decades, NEA/OECD has promoted several projects to the development and application of BEPU methodologies, notably

- UMS (Uncertainty Methods Study) Project, developed from 1996 to 1998.
- BEMUSE (Best estimate Methods – Uncertainty and Sensitivity Evaluation) Project, developed from 2004 to 2009.

The NEA/CSNI/R(2007)9 Report [11] on Safety Margin Action Plan (SMAP) discussed the concept of safety margins involved in the analysis of AOO and DBA. Based on the concepts there developed, Figure 1.2, taken from [17], illustrates the relation between calculated results and the acceptance criteria when performing BEPU.

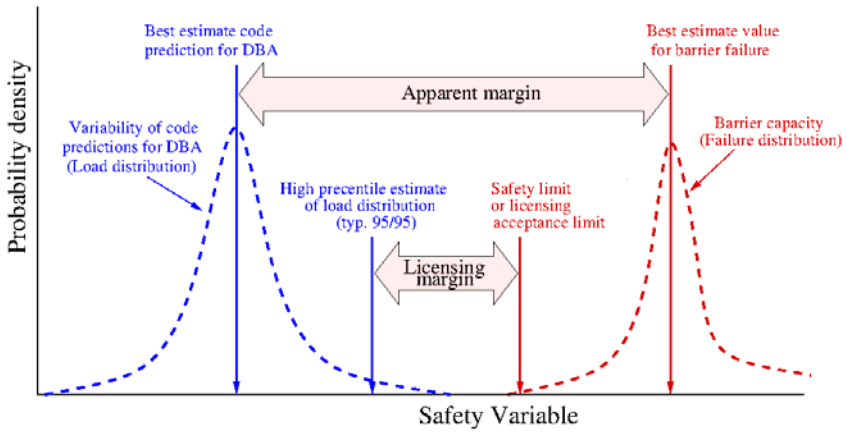

Figure 1.2: DBA analysis outcome (load) and barrier failure (capacity) distributions [17].

The figure illustrates that the difference between peaks of both distributions can be termed the “Apparent margin” (other possible definition could involve the difference between median values or mean values of both distributions). The difference between the upper tolerance limit (typically 95/95) and the licensing acceptance limit can be termed “Licensing margin”. Any distance between relevant values of the safety variable in Figure 1.2 might be termed “Safety margin” since all of them represent margins involved in the safety analysis. However, since the Licensing margin is the one providing the criterion for safety acceptance of the analysis we will often refer to it as “the Safety margin” throughout this study. It is important to notice that, in general, the higher the licensing margin so defined, the higher the probability that the code prediction does not surpass the barrier failure value.

2. The place of E-BEPU in the safety analysis environment.

2.1. The role of safety systems.

Achieving an acceptable level of safety in a given plant requires, among other things, implementing an adequate level of protection in the form of dedicated safety systems. These systems, when activated, try to drive the plant dynamics towards a safe state. Safety systems activation is demanded when process variables or combinations thereof reach pre-established criteria which are indicative of a disturbance that could result in a non-safe dynamic state. Some safety systems generate shutdown signals to normal operation systems while others are stand-by systems ready to start-up when needed. The level of safety of the plant strongly depends on the design of safety systems, including their actuation criteria, and the ultimate goal of the safety analysis is to verify that the risk derived from the facility is as low as reasonably practicable and, in any case, below established limits.

The purpose of the safety systems is a) to prevent the escalation of the initial disturbance to a more severe situation and b) to mitigate the effects of harmful phenomena that could occur in such an abnormal situation. As a general rule, safety systems actuation is triggered by automatic signals. Automatic initiation criteria and capacity are essential points of their design. However, operation of safety systems may imply also some undesirable side effects and their initiation should be avoided unless really required. This makes necessary to optimize the design of safety systems, so that their actuation is demanded if and only if necessary. This is a difficult task which requires very sophisticated methods.

Risk from nuclear power plants mainly comes from their potential to produce harmful radiological effects on people or environment. A limited risk results from limiting the likelihood of exceeding established dose limits. As it is well known, successive protection barriers are provided to avoid the dispersion of radioactive material, hence its consequential radiological effects. Maintaining barrier integrity or, at least, limiting their degradation is the primary purpose of safety systems although the ultimate goal is to avoid unacceptable radiological effects. Barrier challenge is measured by suitable safety variables which are process variables or functions of process variables. Keeping safety variables within specified limits, called safety limits, ensures that barrier degradation will be kept within acceptable limits. This way, the purpose of safety systems can also be stated in terms of avoiding exceedance of specified safety limits.

2.2. Design basis of automatic protection

In nuclear power plants, most of the safety systems are initiated automatically when plant process variables fulfil some criterion implemented through one or more pre-defined set points. There could be several initiation set points and, in some cases, the same set point generates initiation signals for several safety systems. In any case, the capability of safety systems to avoid exceedance of the safety limits will depend on the fulfilment of the design assumptions and the correctness of the initiation set points. Since it is not practical to develop actuation set points conditional to any possible plant state and abnormal event, the first task in the design of safety systems is to determine their design basis, i.e., which types of abnormalities require the successful intervention of those systems and which can be regarded as being beyond their design basis.

Candidate scenarios to be included under the umbrella of automatically actuated safety systems are those that require a fast and accurate response to remediate the situation or those that occur very often. Scenarios typically beyond the scope of the automatic safety systems include those involving multiple, independent failures or unanticipated operational conditions. In all cases, scenarios that are outside the design basis should be very unlikely and, in general terms, the more scenarios included within the design basis, the higher the resulting level of safety.

The great variety of adverse situations that require intervention of safety systems makes unfeasible to apply the same safety limits for any kind of scenario. Depending on the severity and the likelihood of a given scenario, the applicable safety limits may vary and the acceptable level of barrier degradation could be different. For this reason, the whole set of accidental scenarios included in the design basis is usually divided in different classes of accidents with different applicable safety limits and possibly different requirements and design assumptions. The number and names of the accident classes may vary among regulatory systems or design standards but it is quite usual to define three main classes of accidents:

a) Frequent and very low severity faults where no safety limit exceedance is allowed, hence any consequential barrier degradation is prevented.
b) Infrequent but not rare events that could result in some safety limit exceedance and consequential limited barrier degradation.
c) Rare events where some barriers could be significantly damaged but not totally destroyed.

Each class of accidents provides design basis for specific safety systems although any safety system will be credited for accidents of any class if needed. For example, the capability of the safety injection system of a PWR is designed to mitigate loss of coolant accidents; however, this system is also used to maintain the reactor coolant volume in cool-down accidents, e.g., steam line break or opening of steam valves, although the initiation criteria will be possibly different.

Design methods require reducing the virtually unlimited number of scenarios grouped in each class to a small number of transients[1] (or accidents) that represent the whole class. These representative transients must be selected with the criterion of maximizing the challenge to the involved safety systems. This way, the selected transients configure an envelope of the class so that, if effectiveness of safety systems is demonstrated in this reduced number of bounding transients, it gets guaranteed for any transient belonging to the class. Design specifications of safety systems are, therefore, based on this reduced set of bounding transients and, for this reason, they are usually referred to as *design basis transients* (DBT) or *design basis accidents* (DBA). The set of all the DBTs is known as the *design basis envelope* (DBE).

Identifying a realistic transient as the most limiting case for performance of one or more safety systems is not an easy task. Instead, design methods allow for defining a DBT using unrealistic assumptions or parameters that magnify the challenge to safety systems while maintaining the essence of the realistic transients it tries to bind. Because of that, DBTs are qualified as *postulated transients*. The analysis or the simulation of a DBT does not show how the plant behaves; rather, it shows a boundary that the plant behavior will never reach in real cases matching the design basis assumptions.

2.3 The two levels of protection verification

Once the safety systems have been designed, it is necessary to verify their adequacy and sufficiency. Safety systems will be adequate if they are able to maintain the dynamic plant state within applicable limits when disturbances remain within the design envelopes. Safety systems will be sufficient if they provide enough level of safety to the plant, i.e., if the likelihood of exceeding established limits is low enough. This double verification is performed in two steps or verification levels that, although typically based on different methods and assumptions are not independent of each other.

[1] The terms *scenario*, *transient* and *accident* will be used interchangeably throughout this document. Accordingly, *Design Basis Transient* (DBT) and *Design Basis Accident* (DBA) will be used as synonyms.

The first level focuses on the safety system design itself. It is aimed at verifying that safety systems perform as expected when they have to interact with the rest of the plant and among themselves and, therefore, they are able to maintain barrier degradation within required limits[2]. To this aim, this verification level should include verification of the envelopes, verification of the accident classes and their frequencies and verification of the capabilities of the safety systems. Additionally, it must be verified that, with the allowed level of barrier degradation, radiological limits are not exceeded.

Verification of envelopes consists of confirming that any transient that is expected to be within the design envelope is actually there. This occurs if the smallest margins to applicable safety limits are those observed in Design Basis Transients i.e., if any other transient matching the design basis assumptions does not result in dynamic plant states with smaller safety margins.

Verifying envelopes involves a high level of complexity and lacks well established methods to achieve the goal. However, as new analytical tools and techniques are developed, some degree of systematization can be introduced for verification of envelopes. For example, the use of sensitivity and uncertainty analyses in safety assessments allows for a limited but systematic searching for possible transients that are outside the design envelope. Also, some risk analysis methods, although mainly intended for the second level of verification, may provide useful information about the correctness of design envelopes since they could help finding transients, matching the design basis requirements, where some limit is exceeded.

Frequency verification of accident classes, i.e., checking for possible excess of accumulated frequency within a single class is not usually performed or, at least, it is not visible. Only when reclassification of a particular DBT is proposed, there are frequency analyses supporting the proposal. However, the focus is only on the frequency of the DBT itself or, more exactly on the frequency of the initiating event. Frequency accumulation effects are not usually addressed.

The last part of the first level of safety verification consists of checking the safety system performance. Once the envelopes are verified, i.e., when the DBT are confirmed as the most demanding challenges for safety systems, the evolution of safety variables in these transients is calculated and compared to applicable safety limits to confirm that none of them is exceeded or, at least, that the exceedance probability is within acceptable tolerance limits.

Verification of safety system performance is typically addressed with deterministic methodologies and, because of that, this task along with its complementary verification of radiological consequences, is frequently named Deterministic Safety Analysis (DSA). In most regulatory systems, particularly those following the USNRC model, this is the only part of the first level of safety verification that is included in SAR. In this regulatory scheme, Chapter 15 of SAR contains the main results of the DSA, i.e., of the DBT analysis. In addition, Chapter 6 contains containment response analysis for DBA LOCA and MSLB.

The second verification level can be seen as a global assessment of the plant safety which takes into account any potential for damage generation. Consistently, any protective feature, not only safety systems, should be taken into account in this verification level. For example, operator actions required by emergency procedures may play a fundamental role. Moreover, any type of disturbance, not only those matching the assumptions of the protection design basis and any type of subsequent failure, should be considered.

Typically, the second level verification is addressed using probabilistic methodologies, which implement codes that apply probability theory to calculate risk measures. Actually, classical PSA falls in this category. Nevertheless, probabilistic methodologies need to define success

[2] Although the main focus of the first level verification is on automatic safety systems, some operator actions are very seldom credited.

criteria for safety functions, most of them related with performance of safety systems. This is why the first level verification is a prerequisite for the second level. On the other side, an unfavorable result of the second level verification could lead to a revision of the design of safety systems.

2.4 Where is E-BEPU located in this panorama?

E-BEPU is a methodology intended for first level verification. As such, it is oriented to the analysis of design basis envelopes and it therefore focuses on the analysis of postulated DBT. However, it cannot be strictly considered a deterministic methodology since it incorporates significant risk insights into this analysis.

As indicated by its name, E-BEPU can be seen as an extension of existing BEPU methodologies developed to incorporate uncertainty analysis in the verification of safety system performance. Although uncertainty is typically (and most frequently) modelled through probabilities, BEPU methodologies are still considered deterministic methodologies. They address uncertainties in model parameters, initial conditions and some boundary conditions but the scenarios to be analyzed are still deterministically postulated. Furthermore, the predictive models/codes involved in BEPU are deterministic, in the sense that, when they are repeatedly applied to a given set of input values, they produce always the same output values. Any analysis scenario starts with a *Postulated Initiating Event* (PIE) and the subsequent evolution is determined by a postulated sequence of events which includes the most unfavorable single failure on demanded safety systems. In some cases, two or more variants of the scenario are analyzed, but all of them are postulated.

The scope of uncertainties is enlarged in E-BEPU by including scenario uncertainties. This means that only the initiating event and some analysis assumptions are postulated. On the other side, random failures are included in the analysis making the scenario uncertain. This uncertainty, additional to the usual BEPU uncertainties, is addressed through event tree / fault tree techniques similar to those of PSA. Each PIE gives rise to an event tree whose branching probabilities are calculated with fault trees. Every individual event tree must produce acceptable results for considering acceptable the E-BEPU analysis. This is an important difference with respect to PSA where the analysis results consist of the aggregation of the results of all the event trees.

Among the advantages of E-BEPU with respect to traditional DSA methodologies it can be mentioned that it improves the verification of design envelopes due to the systematic introduction of variants of the design scenarios that can reveal weaknesses of the DBT. Defence-in-depth aspects of the protection design are also better addressed with E-BEPU. These points will be further developed in subsequent chapters of this document.

In summary, E-BEPU is an integrated deterministic-probabilistic methodology intended for verification of the protection design (first level verification), which is the traditional field of DSA. It incorporates PSA techniques which convert each DSA DBT in an event tree initiated by a PIE. Contrary to PSA where the results of all the event trees are aggregated, E-BEPU event trees are individually evaluated and compared with acceptance criteria.

3. Basis for the introduction of Extended Best Estimate plus Uncertainty (E-BEPU) methodology

Every nuclear operator wants optimum plant utilization and extended operational flexibility which can only be achieved by the gain in margins i.e. by demonstrating, with the use of improved analysis methodologies, that safety margins are in reality bigger than proved by previous computational analyses and, therefore, can be reduced. In addition, excessive margins often imply that protective actions, usually aggressive, could be unnecessarily initiated, contributing to degradation processes in the long term. Thus, both for operational flexibility and for safety reasons, although safety margins must be always preserved, it could be advisable to reduce them when they are too large. For this reason, a number of efforts is underway in many countries in order to develop new more realistic approaches allowing for a more accurate assessment of safety margins.

Extended BEPU methodology aims to achieve similar impacts i.e. demonstrate the existence of bigger safety margins that could be utilized for bigger operational flexibility or plant modifications for power uprates, design life extension and similar. However, at the same time, E-BEPU allows for introduction of new criteria oriented to better address other aspects of the plant safety such as defence-in-depth or robustness of the safety design (mainly, avoidance of cliff-edges) for which traditional methods are weaker. In addressing sequences that fulfil the regulatory acceptance criteria with STL, additional, more stringent requirements are placed in order to eliminate any possibility for cliff-edge effects. On the other hand for certain sequences that do not fulfil the RAC with STL but have low enough probability of occurrence, reclassification into a higher class is allowed, where they are compared to the acceptance criteria of that class (or some other more stringent criteria) but with a stricter, new level of acceptance. The “single failure criterion” is mandatory, according to the current licensing bases, in the design of safety systems as a vital constituent of defence in depth. However, in the design verification analysis with E-BEPU, it is to some extent relaxed (not eliminated) while, on the other hand, combination of failures, sometimes more likely and potentially more harmful than the worst single failure, are taken into consideration.

The common feature of the conservative, BE and BEPU analysis is that conservative assumptions are made about the availability of safety systems (See the Table 1.1). The single failure criterion stipulates that the safety related systems shall be able to perform their safety function also in the event of any single failure. This principle can be applied either to safety systems composed by redundant trains or to diverse systems designed to perform the same safety function. The following discussion will focus on the case of systems with redundant trains but the same considerations can be done for diverse systems. In applying this principle to the deterministic analysis of a two-train safety related system, one train is conservatively assumed to be unavailable. In other words, the probability that a particular train of a safety system is available can only take two values, namely 1 or 0 and there must be one train assumed failed, i.e., with 0 probability. The main point of E-BEPU is to provide more realistic and more flexible solution by quantifying the probability that a certain train will be available or unavailable and not simply assigning the probability to 0 or 1. Different combinations of available safety system trains are analyzed and adequately weighted with their respective probabilities.

This approach is not completely new. The same idea has been proposed already in the US standard ANSI/ANS-51.1 [13] and German standard KTA-SG-47 [14]. Both standards bring the idea that for certain sequences coming from the same postulated initiating event (PIE), different acceptance criteria can be applied, given that their conditional probability of occurrence is low enough. Based on their conditional (given the occurrence of the PIE) probability of occurrence sequences can be classified in different plant states (PS) where different acceptance criteria may apply for different parameters.

Another very important point to highlight is that the main features of E-BEPU make it highly consistent with the newest IAEA Safety Requirements on Design of NPPs, SSR 2/1 Rev. 1 in its Requirement 42 para 5.73 which requires that **safety analysis shall provide assurance on safety margins, avoidance of cliff-edge effects and early and large radioactive releases.** Demonstration of available safety margins and assurance that there are no cliff-edge effects is explicitly addressed in the E-BEPU methodology.

3.1. Safety analysis of the plant design

The top level IAEA standard Fundamental Safety Principles SF-1 [3] sets the high level requirements for the performance of deterministic safety analysis in its Principle 8 on Prevention of accidents where it is stated that "all practical efforts must be made to prevent and mitigate nuclear or radiological accidents" (note that in the most recent IAEA publications word "accidents" is being replaced with the word "emergencies"). In order to comply with this principle and consequently to ensure that the likelihood of an accident having harmful consequences is extremely low, measures need to be taken:

- "To prevent the occurrence of failures or abnormal conditions (including breaches of security) that could lead to such a loss of control;
- To prevent the escalation of any such failures or abnormal conditions that do occur."

Further, in the next paragraph, SF-1 establishes that the primary means for preventing and mitigating the consequences of accidents is the application of the concept of defence-in-depth (DiD). "Defence-in-depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level of barrier would be available. When properly implemented, defence-in-depth ensures that *no single technical, human or organizational failure could lead to harmful effects, and that combinations of failures that could give rise to significant harmful effects are of very low probability".*

Underneath the Safety Fundamentals are Safety Requirements which prescribe the way that the fundamental safety principles are achieved. The IAEA Safety Requirement SSR 2/1 (Rev 1) sets the requirements for the performance of safety analysis of the plant design in its Requirement 42. It requires a safety analysis of the design for the NPP to be conducted in which deterministic safety analysis and probabilistic safety analysis shall be applied to enable the challenges to safety in the various categories of plant states (PSs) to be evaluated and assessed.

SSR 2/1 req. 42 para 5.71 requires that based on safety analysis, the design basis for items important to safety be established. Further, para 5.71 requires that design shall comply with authorized limits on discharges and dose limits in all operational states. Even more precise requirement is stipulated in European Utility Requirements (EUR) Chapter 2.1.9.2 Table 3 [15] where frequencies and general acceptance criteria for all plant states are presented.

SSR 2/1 Req. 42 para 5.72 requires that safety analysis shall provide assurance that defence-in-depth has been implemented in the design of the plant.

SSR 2/1 Req. 42 para 5.73 requires that safety analysis shall provide assurance on safety margins, avoidance of cliff-edge effects and early and large radioactive releases.

SSR 2/1 Req. 42 para 5.74 requires that the applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design.

SSR 2/1 Req. 42 para 5.74 provides the requirements for deterministic safety analysis in 6 points (a) to (f):

(a) Establishment and confirmation of the design bases for all items important to safety;
(b) Characterization of the postulated initiating events that are appropriate for the site and the design of the plant;
(c) Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements;
(d) Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection;
(e) Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator;
(f) Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator.

EUR Chapter 2.1.4.2 on deterministic safety analysis gives requirements in its subchapters 2.1.4.2.1, 2.1.4.2.2 and 2.1.4.2.3 which go beyond the SSR 2/1 Req.42.

In 2.1.4.2.1 on general principles it defines acceptance criteria, safety objectives and targets for all plant states. It further defines “safe state” following AOO, DBA and Complex sequences and “severe accident safe state” and requires that safe state shall be reached within 24 hours following AOO and DBA. For Complex sequences it recommends (“should” statement) to reach the safe state within 24 hours and, in any case, it requires (“shall” statement) it to be reached before 72 hours. The severe accident safe state shall be reached within 7 days following severe accidents. Such numerical targets go far beyond requirements in IAEA Safety Standards but are extremely useful for deterministic safety analysis practitioners.

In 2.1.4.2.2, rules used in performing deterministic safety analysis are prescribed, such as use of single failure criterion and requirement to postulate LOOP with each initiating event when analyzing AOO and DBA. This again goes beyond requirements in the IAEA Safety Standards but can be found in lower level documents such as Safety Report Series # 23 “Accident analysis for NPPS”.

In 2.1.4.2.3 defines deterministic safety analysis methodologies. For AOO and DBA three options are available: full conservative analysis with conservative codes and conservative initial and boundary (I&B) conditions, best estimate (BE) codes and conservative I&B conditions and BE with evaluation of uncertainties (BEPU). For DEC it is suggested to use only BE approach due to large uncertainties. IAEA Safety Guide SSG-2 on Deterministic Safety Analysis supports such analysis methodologies. In addition to three listed methods; conservative, BE and BEPU, the SSG-2 also introduces the so-called Option 4 or Extended BEPU that included BEPU plus the treatment of the availability of safety systems in a probabilistic manner which is the subject of this study.

SSR 2/1 Req. 42 para 5.76 sets the requirements for probabilistic safety analysis. It states that the design shall take due account of the probabilistic safety analysis of the plant for all modes of operation and for all plant states, including shutdown, with particular reference to:

(a) Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent;

(b) Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented;
(c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

More precise guidance on the application of probabilistic safety analysis is given in the IAEA Safety Guides SSR-3 [6] and SSR-4 [7].

The next two sub-sections will briefly introduce the latest international requirements for PIEs and PSs as those will be referred to throughout this study.

3.1.1. Postulated Initiating Events (PIEs)

For PIE, SSR 2/1 [4] stipulates in its Requirement 16 calls for identification of a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design. Further, under the same Requirement 16 in paragraphs 5.5 – 5 15 more details conditions are set for PIEs:

SSR 2/1 para 5.5 calls for the use of engineering judgement and a combination of deterministic and probabilistic safety assessments in identification of PIEs.

SSR 2/1 para 5.6 requires that PIEs include all foreseeable failures of SSCs as well as operator errors and possible failures arising from internal and external hazards in all modes of plant operation.

SSR 2/1 para 5.7 requires that an analysis of the PIEs be made to establish the preventive and protective measures necessary for the assurance of required safety functions.

SSR 2/1 para 5.8 lists the expected behavior of the plant in any PIE in order of their priority.

SSR 2/1 para 5.9 requires grouping of PIEs when used for developing the performance requirements for the items important to safety.

SSR 2/1 para 5.10 requires a technical justification for exclusion from the design of any PIE that has been identified.

SSR 2/1 para 5.11 calls for the automatic safety actions for the actuation of safety systems when prompt and reliable actions would be necessary.

SSR 2/1 para 5.12 deals with operator actions in response to PIE which do not need a prompt response.

SSR 2/1 para 5.13 requires that capability to monitor the status of the plant be available.

SSR 2/1 para 5.14 requires equipment and procedures to be available for keeping control over the plant and for mitigating any harmful consequences.

SSR 2/1 para 5.15 requires any equipment for which manual action is required to be placed in the most suitable location to ensure its availability at the time of need and to allow safe access to it under the environmental conditions anticipated.

3.1.2. Plant states (PSs)

Plant states that are considered in the design of nuclear power plants are defined in a similar way in all international standards but with different titles/names and it is therefore prudent to show the equivalence among different definitions.

In the European Utility Requirements (E.U.R.) [15], IAEA SSR 2/1 [4] and in WENRA Safety of new NPP designs [16] the initial states are identical:

Normal operation (NO)

Anticipated operational occurrences (AOO)

For design basis accidents (DBA) and design extension conditions (DEC) Table 3.1 shows different names used for the corresponding conditions:

E.U.R.	IAEA	WENRA Safety of new NPP designs
Design Basis Accidents	Design Basis Accidents	Postulated single initiating events
DEC – Complex sequences	DEC-A without core melt	Postulated multiple failure events
DEC – Severe accidents	DEC-B with core melt	Postulated core melt accidents

Table 3.1: Nomenclature for DBA and DEC in different international standards

For the purpose of classifying the postulated initiating events, the plant conditions for DBA are categorized in the following way:

Normal Operation as – Design Basis Condition 1 = DBC1

Anticipated operational occurrences as – Design Basis Condition 2 = DBC2

Design basis accidents with frequency of 10^{-2} – 10^{-4} as – Design Basis Condition 3 = DBC3

Design basis accidents with frequency of 10^{-4} – 10^{-6} as – Design Basis Condition 4 = DBC4

Even though the names and the frequency values may vary among different standards, the concepts are the same in all international standards and requirements.

3.1.3 Acceptance Criteria for Plant States

Acceptance criteria for different plant states are essential in the application of E-BEPU as it is often necessary to compare fulfilment of the acceptance criteria for the class of the PIE with a standard tolerance level (STL) and the fulfilment of the acceptance criteria for the next class with a different tolerance level.

The acceptance criteria are usually prescribed by the regulatory body for different plant states in different categories both at radiological level and barrier integrity level. Barrier integrity level criteria, which are the relevant ones for E-BEPU, are most commonly prescribed for:

- General plant condition
- Fuel and cladding
- Reactor coolant system
- Primary containment
- Spent fuel pool
- Off-site radioactive releases

To demonstrate the acceptance criteria on barrier integrity for a pressurized water reactor (PWR) plant we take the example of “fuel and cladding”:

- For DBC1 – fuel elements operate below specified acceptable fuel design limits
- For DBC2 – no fuel damage allowed, with 95/95 probability and confidence departure from nuclear boiling (DNB) does not occur on any fuel rod surface
- For DBC3 – only minor fuel damage allowed, less than 5% of fuel rods experience DNB
- For DBC4 – the postulated initiating event (PIE) shall not result in consequential damage of the reactor coolant system (RCS) or result in the loss of a safety function
- For DEC-A – the PIE, including the additional failures, shall not result in consequential damage of the RCS
- For DEC-B – the only criterion is that the containment integrity shall be maintained, as the core has melted and the integrity of the last barrier is required.

Similar acceptance criteria can be found in the national regulations of all countries operating NPPs for other categories.

3.2. The progression through DSA analysis options

The evolution of the rules applying to DBA analysis reflects the need to make compatible two essential characteristics of the plant protection. First, and most important, safety analyses focusing on DBA must be bounding or enveloping analyses since the objective is to support the design of SSC important to safety and demonstrate, from the analysis of a relatively small number of cases, that the plant is adequately protected in a great variety of possible real situations. This implies that conservatism is an intrinsic characteristic that must be preserved in this type of analysis. Second, protective actions must be commensurate with the safety significance of the plant states where those actions are triggered. Unjustified initiation of protective actions is not only a disturbance of the production process but also a safety problem due to the undesirable side effects that sudden changes in the plant sate may produce. Optimization of the plant protection design consists of ensuring, to the extent possible, that protective actions are initiated whenever they are needed but only in those cases.

At the beginning of nuclear safety regulation, the need to preserve conservatism was clearly dominant. Lack of detailed knowledge of some physical phenomena and poorly efficient computer codes forced to impose strictly conservative criteria to the analysis of design basis accidents. At the same time, lack of reliability data and limitations in the computing power made inevitable the use of deterministic assumptions like the single failure criterion on the configuration of safety systems. For the great majority of the transients and accidents analyzed in Safety Analysis Reports, designer methods based on verified conservative assumptions and models were accepted by regulators. For the special case of LOCA accidents, the USNRC issued Appendix K of 10 CFR 50, prescriptive in nature, which was widely adopted among the international nuclear community.

As a result of continuous research on physical phenomena occurring in nuclear power plants along with a permanent effort in developing more accurate, efficient and reliable computer codes, it was possible to reduce conservatism in the analysis while ensuring maintenance of enough safety margins. As reflected in the IAEA Safety Guide SSG-2, new analysis options were possible.

Transition from Option 1, represented by Appendix K, to Option 2 consisted of reducing conservatism in simulation models. Best estimate computer codes had been developed and sufficiently validated as to make them usable for safety analysis. However, the capability of realistic models to adequately represent reality depends on the use of adequate values for model parameters. In many cases, these parameters are not accurately known and the required conservatism of safety analyses leads to using bounding values for those parameters, more pessimistic than any possible realistic value. The specification of the analysis cases in Option 2 continued to include conservative safety system configurations.

With the dramatic increase in computing power, started in the 80's and still continuing today, it was possible to open new possibilities to reduce unnecessary conservatism. One of the problems of Option 2 was that it could be difficult to find bounding values of some parameters. In some cases, the range of uncertainty was so large that any bounding value became too unrealistic. In other cases, the worst value of a parameter was not any of the extremes of the uncertainty range but some intermediate value, difficult to identify. This type of difficulties could only be solved with a more detailed accounting of uncertainties, thus requiring a significant increase in computing resources.

The issuance by the NRC of the revised rule for LOCA/ECCS analysis, 10 CFR 50.46 in 1989, definitely opened the door for BEPU methods in the United States but also as a reference at international level. The release of the revised rule was accompanied by that of Regulatory Guide 1.157 (a best estimate counterpart to Appendix K) and of CSAU (Code Scaling, Applicability and Uncertainty) Evaluation Methodology, which can be regarded as the first Option 3 methodology. Option 3 of IAEA SSG-2 refers to the different methodologies that have been developed with the premises of relaxing some of the constraints of Option 2 with regard to conservatism of simulation model parameters and, in some cases, of initial and boundary conditions. The use of more realistic parameter values was compensated with a detailed uncertainty analysis.

Even though the main purpose of moving from Option 2 to Option 3 was to better characterize safety margins and allow for their reduction in case they are shown large enough, the new methods allowed for a clear improvement of some aspects of the analysis. For example, it has been mentioned that bounding values of model parameters are not always at the extremes of the uncertainty range; in addition, it can be found that identifying the worst values of individual parameters is not equivalent to identifying the worst combination of parameter values. These and other types of problems could not be adequately addressed with Option 2 methods. In Option 3, however, where statistical methods based on random sampling are widely used, bounding values of individual parameters and bounding combinations of parameter values are automatically considered and weighted.

In Option 1 and Option 2, exceedance of applicable safety limits in DBT/DBA was not allowed at all. Transition to Option 3 changed the strict compliance with regulatory acceptance criteria by less stringent criteria such as the use of tolerance levels. The revised ECCS rule (10 CFR 50.46) required basically a probabilistic modelling of uncertainty for LOCA/ECCS results. Based on that, the fulfilment of RAC in Option 3 is not demanded strictly, but with a high enough probability and a high enough statistical confidence. The pair formed by probability and statistical confidence is termed statistical tolerance. Then, RAC must be satisfied with a high level of tolerance, such level being established by the regulatory authority. The change implies that some degree of safety limit exceedance is allowed although the methodology guarantees that this occurs with very low probability. Safety margins, traditionally understood as the difference between two values of a safety variable, one corresponding to a plant state and the other corresponding to a limit, loose their significance due to the uncertainty of the plant state. Instead, a probabilistic concept of safety margin can be defined in terms of conditional exceedance probability of the established safety limits.

The journey from Option 1 to Option 3 consisted of removing conservatism from simulation models and from the data used to feed those models. However, Option 3 still retains significant conservatism in the definition of DBT/DBA, i.e., of the scenarios being analyzed. It is clear that they must be enveloping scenarios involving some degree of conservatism but, as in the case of models and parameters, an excess of conservatism could imply unexpected effects such as masking other safety problems. In Option 3 and its predecessors, the analysis scenario is defined by a Postulated Initiating Event (PIE) and a fixed configuration of safety systems, along with other possible concurrent events such as LOOP. In determining the configuration of safety systems, the single failure criterion plays a fundamental role.

As a natural continuation of this evolution, Option 4 represented by E-BEPU tries to remove some of the conservatism in the definition of analysis scenarios. The main change is to consider the availability of safety systems as an additional uncertain element of the analysis. This implies that different configurations of safety systems should be taken into account instead of considering only the configuration with the worst single failure. As in previous changes of DSA Options, transition to Option 4 is possible because of an increase in existing knowledge and the result is not limited to the intended gain in safety margins.

E-BEPU takes advantage of the huge knowledge base on system reliability developed as a part of the implementation of PSA in practically all the plants throughout the world. Also, some of its methods are borrowed from PSA although the objective is different.

The gained flexibility derived from the introduction of new system configurations, not limited to the single failure one, is complemented by the use of improved analysis methods and requirements that allow for better addressing some points not adequately treated in previous Options. Specifically, the introduction of new acceptance criteria with new tolerance levels, additional to those of standard BEPU, provide capability to assess important issues of defence-in-depth such as the possibility of cliff-edge effects. Additionally, E-BEPU is a natural tool to detect the need for design extensions.

All these advantages are obtained, of course, at the cost of an important increase in computing resources which is, nevertheless, affordable.

Based on the paper published in 2014 [17] the Polytechnic University of Valencia (UPV) has made an effort to demonstrate the use of E-BEPU [26, 27]. It is a good work and certainly an addition to the classical BEPU analysis. In their attempt, they add a new uncertainty to classical BEPU, consisting of configuration uncertainty. Then they sample the configuration as an additional uncertain parameter and focus on the most probable configurations, which are necessarily those without failure. In conclusion they find that their results show larger margins than obtained by traditional BEPU analysis. It is a good demonstration that it is possible to go beyond the traditional BEPU, however they don't address in these papers the most important elements of E-BEPU that is comparison with the next class acceptance criteria for detection/avoidance of cliff-edge effects on one hand and reclassification of sequences with very low probability into the next class on the other end.

Several vendors, utilities or technical support organizations are currently working on means to more accurately assess safety margins to licensing limits. Their methods might be different from the one used in E-BEPU but the main objectives are the same to more accurately assess available safety margins which can then be used for better operational flexibility, power uprates, extended fuel cycles or plant aging issues. One such initiative is the ARITA project carried out by Framatome, which is a realistic new approach to non-LOCA safety analysis for application to pressurized water reactors. It assumes a more realistic assessment of the behavior of the reactor system under accident conditions [12]. There are of course also numerous other initiatives which will produce results in the near future. What they all have in common is that they strive towards elimination of undue conservativism in deterministic calculations but without impact any major on nuclear safety. With better understanding of the physical phenomena obtained from numerous experiments and with better computational tools with reduced computational times it seems to be possible to

address these issues. In this regard E-BEPU can be seen as yet another method that could contribute to reduced conservativism in safety analyses by reclassifying the list probable sequences on one hand while placing more strict requirements on more frequent sequences on the other hand.

4. Description of Extended Best Estimate plus Uncertainty (E-BEPU) methodology

No matter which of the DSA analysis options described in 1.3 above is used, the design verification analysis is performed at individual PIE or DBA level. This means that each PIE or DBA must be individually analyzed and compared with the corresponding acceptance criteria. All the analyses of individual PIEs or DBAs must comply with their corresponding acceptance criteria and in no way deficiencies in the analysis of a PIE or DBA can be compensated by favorable results of another one. Analyses of different PIEs are independent of each other, even to the point that it could be acceptable to use different analysis options for different PIEs, e.g., some of them analyzed with Option 3 (BEPU) methods and others analyzed with Option 4 (E-BEPU). This chapter describes how the E-BEPU methodology is applied to an individual PIE. This is extended from the work presented in [17].

The use of the E-BEPU methodology for a given PIE is summarized in the flow diagram of Figure 4.1. This is a high level diagram where each block represents a more or less complex set of operations. The following sections are detailed descriptions of each block of the diagram. It should be noted that the present description reflects the current state of development of E-BEPU. It can be expected that some adjustments would be needed as experience is being gained in the implementation process and application exercises.

4.1. PIE classification in E-BEPU (Block 1).

The first step in the E-BEPU analysis of a given PIE is to identify the class to which it belongs. This determines the regulatory acceptance criteria applicable to the analysis of the PIE. Most often, the E-BEPU practitioner will start from an existing accident classification and definition of PIEs. However, it is important to have a clear understanding of the concepts involved in accident classification in order to avoid possible inconsistencies in the application of the methodology. The following description includes a brief discussion on the fundamentals of accident classes and PIEs.

4.1.1. Accident classes for design basis analysis

Classification of accidents is a common characteristic of DSA methods. As described in Section 2.2, accident classes or categories are defined in order to graduate the protective actions and acceptance limits according to the severity and the likelihood of disturbances that take the plant out of a normal operation state. Each accident class is characterized by a frequency range and a specific set of safety limits. An event that may happen randomly along time can be characterized by a frequency, defined as the expected number of occurrences per unit time. It is assumed here that the frequency of an accident is constant along time. The higher the frequency of the class, the stricter safety limits apply, so that anticipated occurrences do not affect barrier integrity and significant barrier degradation is only allowed for very unlikely events.

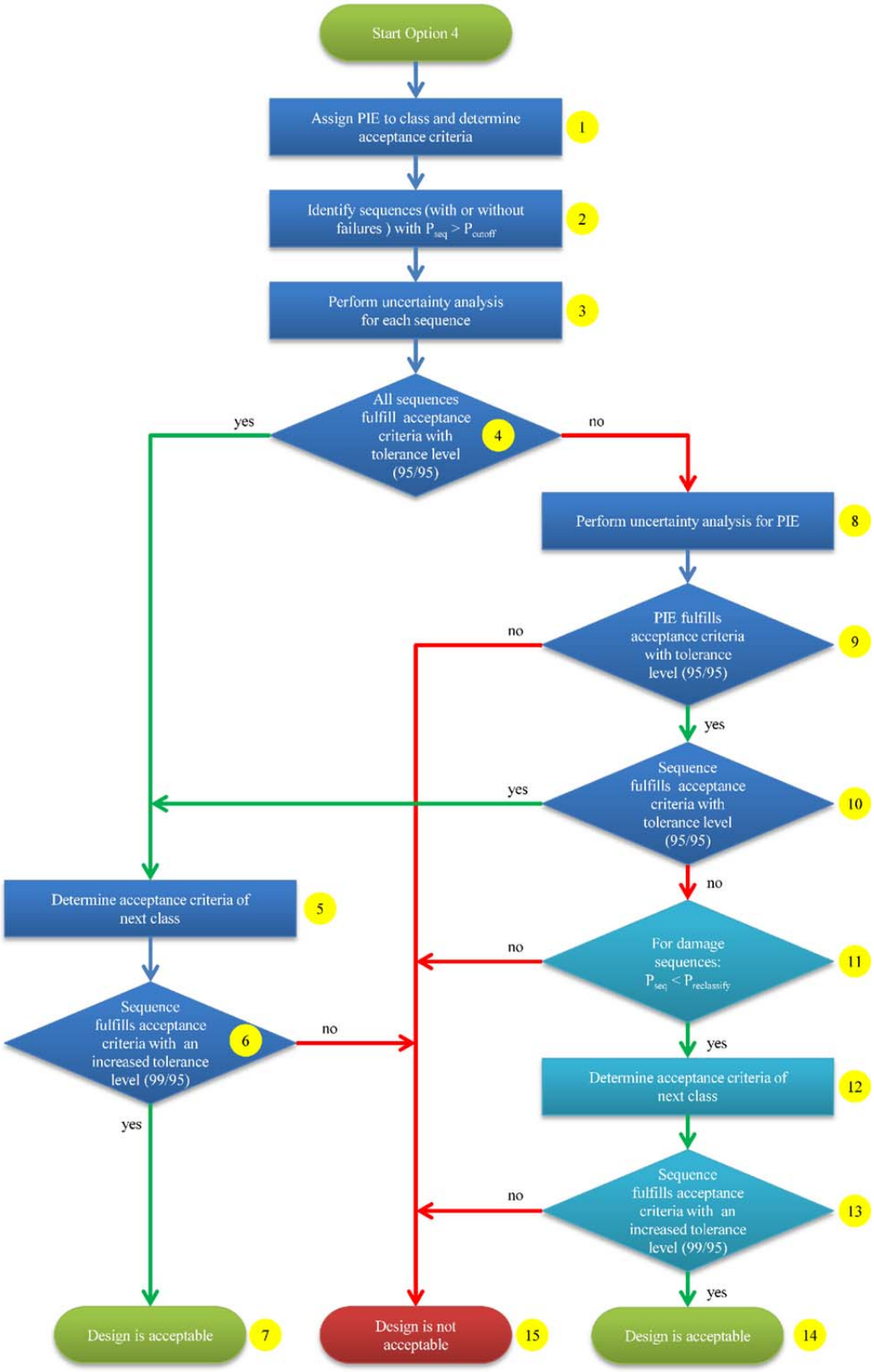

Figure 4.1: Flow Diagram of E-BEPU

Names of accident classes vary from one classification to another. They may be purely descriptive (e.g., Anticipated Operational Occurrences, Postulated Accidents, etc.) but very often they are named by a generic name (Class, Condition, Category), followed by a number.

Those numbers, usually ranging from one to three or from one to four, indicate the relative severity of the class. For example, the very well-known classification of ANSI-N-18.2 [18] defined Condition I to Condition IV accidents, the most severe being Condition IV. We are not adopting any particular classification in this document but in the following discussion, when using terms such as *lower class*, *upper class*, *next class*, *previous class*, we are always assuming that severity is the sorting criterion.

Although the main criterion for accident classification is severity, it is usual to refer to accident classes as *frequency classes*, which could be misleading. In order to understand the meaning of accident classification it is important to distinguish between frequency of an accident and frequency of a damage[3]. A plant can be considered safe if the exceedance frequency function for applicable damage indicators is below specified limits. Figure 4.2 represents a typical exceedance frequency function, also called risk curve, for a generic damage variable D in a given facility.

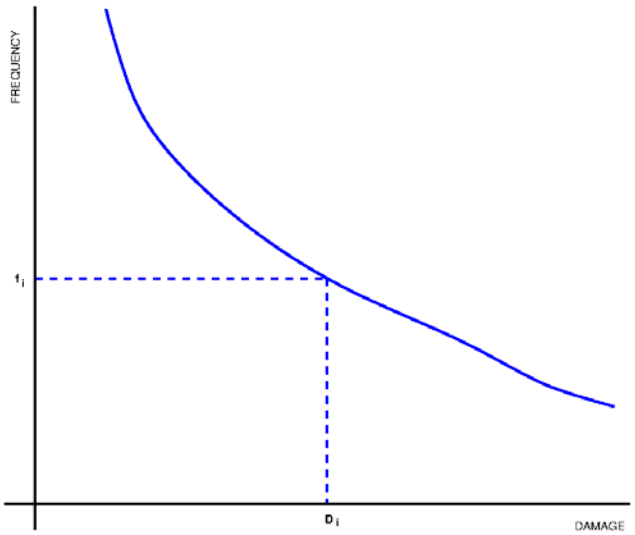

Figure 4.2: Typical risk curve for a generic damage variable

A point of this function represents how frequently (f_i) can be expected that a given level of damage (D_i) will be exceeded due to the occurrence of accidents of any type. Accidents contributing to f_i are those with consequences higher than D_i. The higher the value of D_i, the lower the number of accidents contributing to f_i and, therefore, the lower the value of f_i. We can conclude that, at global plant level, frequency and damage are inversely related. However, there is nothing requiring that the lower the frequency of an accident, the higher its severity. Accidents of high severity should be of low likelihood because, otherwise, they would give an unacceptable contribution to the risk curve. However, mild plant disturbances producing very low or null damage are not required to be highly likely. As for any other type of disturbance, the lower frequency, the better.

Accident classification can be seen as an approximation and discretization of the risk curve. It is an approximation because the classification only includes accidents matching the design basis assumptions. It is a discretization because accidents belonging to a given class are treated as equivalent, so that instead of a risk curve we have a stepped function. Figure 4.3 is a qualitative representation of how the plant risk curve and the design basis accidents classes are related. The red stepped line representing accident classes is necessarily

[3] For the purpose of this discussion the term “damage” means any type of adverse consequence used to measure the severity of accidents, not necessarily a radiological damage. The term “accident” refers to any plant disturbance requiring activation of some protective action.

located below the blue risk curve since accidents outside the design basis contribute to the latter but not to the former.

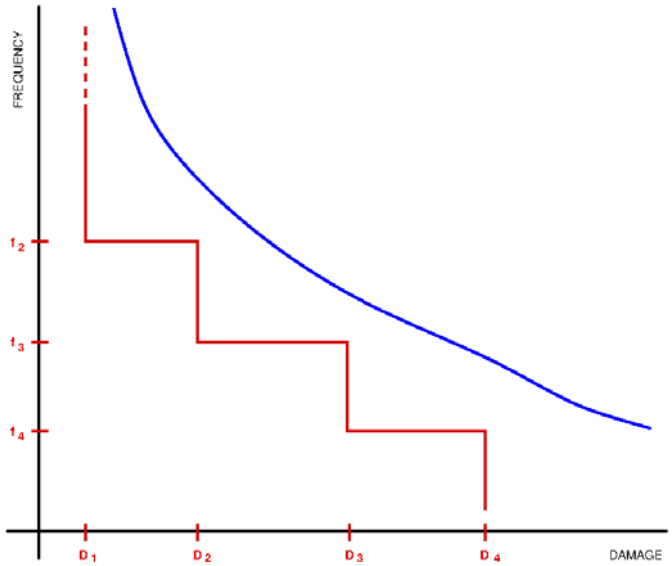

Figure 4.3: Risk curve and Design Basis Accident classes.

Each step of the red line of Figure 4.3 is an accident class. Class i is located to the left of damage value D_i which implies that D_i is an upper bound of the damage generated by any accident of the class. The discretization process consists of assuming that any accident of class i generates an amount of damage D_i. This way, the size of the frequency jump at D_i (i.e., $f_i - f_{i+1}$) is the joint (collective) frequency of all the accidents of the class and the value of the function between D_{i-1} and D_i is constant.

Rules and standards for analysis of DBA define damage limits for each class. If a limit L_i is defined for class i, the maximum damage generated by any accident of the class, i.e., D_i must be lower than L_i. Regarding frequencies, most often accident classes are associated to a frequency range but it is interpreted as a classification criterion according to the frequency of each individual accident, not as a class limit. This interpretation leads to some inconsistencies. For example, let us consider a mild disturbance that can be easily managed to avoid exceedance of any safety limit. If this disturbance is found very unlikely, it should be located in a high class and treated as if it were a very serious accident. This implies, among other things, that the consequences of such a disturbance would be acceptable even if protective actions are relaxed to the point that some safety limits, applicable only to lower classes, get exceeded. Clearly, there is something wrong when it is possible to justify this type of conclusions. Other examples can be found with even more amazing conclusions, like the one outlined in the following paragraph.

Let us assume that an accident, e.g., a particular type of pipe break, with consequences D_a between the limits of class i and class i+1, has a frequency f_a too high as to be classified in class i+1. This unacceptable situation clearly reflects the need to improve the protection design. However, we could decide to divide the range of possible break sizes in n intervals, so that the frequency of breaks within each interval would be f_a/n while the consequences would continue to be D_a. Taking each such break interval one by one and making n high enough, f_a/n would be in the frequency interval of class i+1 where a higher damage limit applies and D_a would be acceptable. The result is that, without changing anything in the plant design, we have converted an unacceptable situation in an apparently acceptable one. This would never be possible if we understand that the class frequency limits refer to the joint frequency of accidents in the class, not to the frequency of individual accidents. In this example, if we quantify the joint frequency of accidents in class i+1 we will find that the

classification is unacceptable because f_a is the same as before and, therefore, too high for class i+1. Once again, it has to be noted that the frequency of a damage is much more safety significant than the frequency of an accident.

Accident frequencies matter, but only as contributors to class frequencies. Of course, if the frequency of a single accident is above the limit of a given class, it cannot belong to that class. However, there is no lower limit for accident frequencies in any class. The only condition is that the accumulated frequency in a single class should be lower than the frequency limit of the class. Surprisingly, this condition is not usually checked.

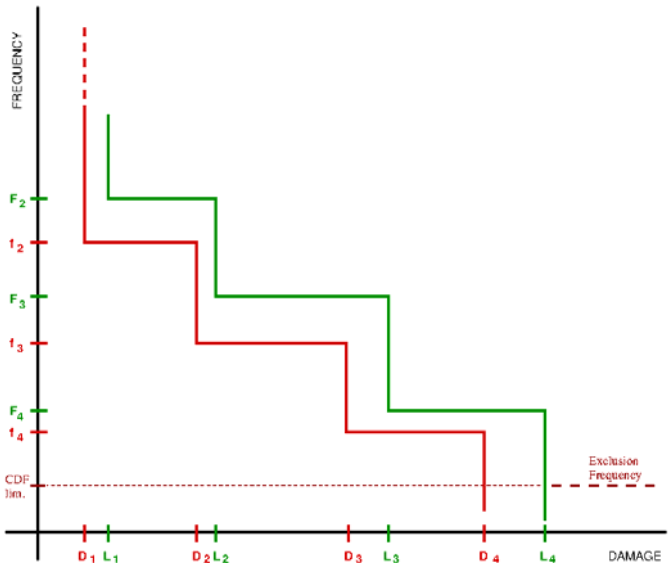

Figure 4.4: Accident classes and their limits.

From the above discussion it can be concluded that a classification of design basis accidents is well defined only if the definition of each class includes a damage limit L_i and a frequency limit F_i. The only exception is that the frequency for Class 1 is not limited because the limit L_1 applies also for normal (continuous) operation where the frequency is unlimited. Figure 4.4 represents the accident classes of Figure 4.3 compared with the applicable limits for each class. Note the difference between D_i and L_i. D_i is a result of the analysis, namely, the maximum value of damage resulting from the analysis of Class i accidents. L_i is an acceptance criterion, i.e., the maximum acceptable value of D_i.

For each class, it is useful and acceptable to replace the damage limit by one or more safety limits that cannot be exceeded. Regarding frequencies, if the classes are qualitatively defined (e.g., “accidents any one of which can be observed during the plant life”) it should be possible to derive approximate values for their frequency limits (e.g., 10^{-2} y^{-1} for the above definition). Otherwise, the classification is not usable in E-BEPU.

Additionally, as shown in Figure 4.4, an exclusion frequency should be defined as the maximum frequency of accidents exceeding the safety limits of the highest class. Both in traditional DSA and E-BEPU it is acceptable, even inevitable, to exclude from the analysis some accidents of high severity if they are found very unlikely. Again, we are talking about collective likelihood of all the excluded accidents. For plants where a limit for core damage frequency is established in PSA, this limit can be used as an exclusion frequency for E-BEPU. Anyway, sequences that are excluded from the design basis analysis are still considered in other types of analysis, e.g., in PSA.

4.1.2 Design Basis Accidents and Postulated Initiating Events

In Section 2.2 above, Design Basis Transients or Accidents (DBA) were defined as limiting analysis cases where safety systems must perform against maximized challenges under the most unfavorable conditions compatible with their design. The set of assumptions used to determine DBAs make them, in many cases, unrealistic. This implies, among other things, that trying to estimate the frequency of a DBA makes no sense. An unrealistic transient has no frequency. Nevertheless, since a DBA is a bounding replacement for a more or less large group of possible real transients, it could make sense to assign to the DBA the collective frequency of that group. The point is now how to estimate the frequency of a large group of transients that are not explicitly identified. Initiating events of DBA may help solving this issue.

In the traditional DSA approach Design Basis Accidents are postulated transients, triggered by a Postulated Initiating Event (PIE). The evolution of the plant state is conditioned by a set of deterministic assumptions that magnify the challenges to barrier integrity and, after the occurrence of the PIE, no additional random event is assumed along the DBA. The worst case philosophy is behind the selection as DBA of one (in some cases, a few) of the possible plant evolutions starting from the PIE which is assumed to envelop all those plant evolutions. This simplifies a little the problem of assigning a frequency value to a DBA. We can focus on the frequency of the PIE for that purpose and, if we are able to assign a frequency to the PIE, we can assign the same frequency to the subsequent DBA.

However, being a postulated event, the difficulties to estimate the frequency of a PIE still remain. The advantage is that the PIE is an event, not a dynamic sequence, and it can be easier to identify what real possible events it is enveloping. It can be expected that a PIE represents all the initiating events of the same type. For example, a PIE defined as “Steam Line Break” in a PWR, hopefully is a replacement for any break in the steam line, at least in a given range. But the envelope could be wider. The immediate effect of a “Steam Line Break” is an excessive core cooling and, under some circumstances, it could be taken as a representative of other over-cooling events such as the over-speed of reactor coolant pumps due to an electric grid disturbance.

How are real initiating events grouped into a set of PIEs depends on specific analysis options, most often decided by designers. It is essential for application of E-BEPU or any other design verification methodology, to know and understand what kind of events are represented by each PIE. This does not solve the problem of estimating the frequency that can be assigned to a particular PIE, but it could help to identify some inconsistencies. It is also essential to make sure that the whole set of PIEs covers the whole set of possible real initiating events.

Fortunately, for the purpose of DSA, it is not necessary to make accurate frequency calculations. It is only a matter of being able to make some consistency checks. Existing classifications may vary in some details but are quite similar and can be considered consolidated. Only if one finds good reasons to question the classification of some PIE, it could make sense to review the criteria. This is so also in the opposite direction: if one wants to move a PIE from one class to another, the arguments must be solid and consistent with the classification philosophy and must comply with the general principle of minimizing damages to the extent possible that can be stated also as “the lower the class of a PIE, the better”.

4.1.3. Additional remarks on PIE classification in E-BEPU

The application of E-BEPU starts, like traditional DSA, from a classification of PIEs. Actually, any valid classification for DSA is also valid for E-BEPU. The class of a PIE determines the RAC to be applied in the analysis. The frequency of the PIE, i.e., the frequency of all the

initiators it represents, added to the frequency of the other PIEs of the same class, must be lower than the limit of the class.

The above discussion about grouping of initiating events into a set of PIEs could suggest that each PIE is a separate entity that can be analyzed independently of other PIEs. This is not completely true because some plant disturbances may involve processes and safety systems that are analyzed in two or more PIEs, not in a single one. An illustrative example is the loss of off-site power in a PWR which is not analyzed as an independent PIE because it is bounded in some aspects by the loss of feedwater and in other aspects by the trip of reactor coolant pumps. In other cases, different ranges of a particular type of disturbance could be represented by different PIEs.

These complexities make difficult to identify with some accuracy what is the set of plant transients bounded by a particular PIE and, therefore, the frequency of the PIE. It can be assured only that the whole set of PIEs bounds the whole set of possible plant transients included in the class. In traditional DSA, once the PIE has been classified, its frequency does not matter anymore and this problem is not relevant. In E-BEPU, however, where further probabilistic evaluations will be performed along the analysis, it is necessary to make some additional considerations about PIE frequency.

The main intend of E-BEPU is to take into account that safety systems may work with different configurations. Determining PIE frequencies with high accuracy is not so relevant for that purpose. Moreover, grouping of initiating events into a set of PIEs is an engineering process which involves some degree of arbitrariness. Different partitions are possible, producing different PIE frequencies. All of them may be acceptable, but the final results of the analysis, i.e., whether the design is acceptable or not, may not depend on the particular solution that has been adopted. For this reason, the relevant fact should be, as in traditional DSA, the class where the PIE is located, rather than its assigned frequency. Again, once the PIE has been classified, its individual frequency should not matter anymore.

In order to ensure that the E-BEPU analysis is class-dependent rather than partition-dependent, every PIE is analyzed as if it were the whole envelope of the class. This means that, for the purpose of the analysis, the frequency assigned to the PIE should be class specific, equal for all the PIEs of the class. The simplest and most enveloping solution is to assign to the PIE the frequency limit of the class (F_i). Then, all the arguments about sequence screening and reclassification that will be described later in this document will be applied in terms of conditional probability (given the occurrence of the PIE) and class frequency limits, but the frequency of the PIE will not be relevant.

4.1.4. Summary of PIE classification for the E-BEPU user

1. Defining a complete set of accident classes and determining the set of PIEs representing each class is a very complex task that exceeds the scope of E-BEPU. It is assumed that the E-BEPU user will start from an existing and widely accepted definition of accident classes.

2. Preferably, the user will choose a classification of accidents where the frequency limits of each class are explicitly defined. Otherwise, it is necessary to determine approximate frequency limits based on class definitions. It should be recalled that, for application of E-BEPU, the relevant frequency values are the upper frequency limits of each class.

3. An exclusion frequency should be defined for accidents exceeding the safety limits of the highest class. Sequence screening is further discussed in Block 2 of the E-BEPU

flowchart. If a limit for CDF exists in PSA, this limit can be used as exclusion frequency in E-BEPU.

4. Accident classes are sorted by severity, lower classes being the less severe ones. For each class, a set of safety limits needs to be defined. These safety limits are the RAC for the accidents of the class.
5. Identifying the class of the PIE being analyzed is the first step of E-BEPU. This determines the acceptance criteria that apply for the analysis of that PIE.

4.2 Sequence identification and screening (Block 2).

Once the PIE class and the applicable RAC have been determined, the next step in the E-BEPU analysis is to identify how the plant state can evolve from the occurrence of the PIE. In general terms, once the PIE triggers a plant transient, one or more safety systems will be required to actuate in order to mitigate the effects of the PIE and to prevent further plant degradation. Additionally some other systems could also be started or stopped as a part of the automatic response of the plant. Therefore, following the initiating event, a sequence of events consisting of system connections or disconnections occurs along the time and determines the plant state evolution.

The request for safety system intervention occurs when some set-point is reached. It should be noted that in the context of design basis analysis, which is the scope of E-BEPU, the plant protection relies on automatic systems. There are very few exceptions where some operator action is credited. Let us consider the general case of automatic systems. Some comments about manual protective actions will be given later.

4.2.1. Safety system demand and intervention

As it is well known, safety systems are, in most cases, composed by a set of redundant trains. When the actuation set-point of the safety system is reached, all the redundant trains receive a request for intervention, although some of them could fail to respond to this request for different reasons. As a consequence, the configuration of the safety system may vary from case to case and not all these configurations could result in an effective implementation of the system safety function. As pointed out in Chapter 2 above, the key feature of E-BEPU is the explicit consideration of uncertain safety system configurations in the analysis.

In some cases, the effectiveness of a required safety function does not rely on redundancy but on diversity. This means that instead of a single system with several redundant trains there could be several non-redundant systems able to achieve the same safety function or another equivalent one. Differences with respect to the case of redundant systems can be significant, for example, diverse systems could have different demand set-points or the subsequent dynamic evolution of the plant state could be very different. However, it still makes sense to talk about safety system configuration as an uncertain issue, the difference being that uncertainty is not stated in terms of how many redundant trains are working but in terms of which safety systems are finally implementing the required safety function.

Following the postulated occurrence of a PIE, intervention of one or several safety systems will be requested but some of them could fail to respond to this request. In traditional DSA, only one among the different failure possibilities is analyzed. The well-known “single failure criterion” consists of deterministically assuming that one and only one failure, additional to the PIE, occurs along the sequence. Among the different possible “single failures” the analyst selects the one producing the worst consequences or resulting in the highest difficulty to comply with the acceptance criteria applicable to the PIE. Only this worst single failure is considered and, therefore, only one sequence starting from the PIE is analyzed in traditional DSA. In this sequence, all the demanded safety systems work in their nominal configuration except the one where the “single failure” is located.

The implicit assumption behind the single failure criterion is that any combination of two or more failures is much less likely than any single failure. Thus, multiple failures are excluded from the analysis and the worst failure is selected on the sole basis of consequences. However, a single failure of very low likelihood opens the possibility of a more likely combination of two failures leading to worse consequences. This possibility is not excluded in E-BEPU where all the possible sequences starting from the PIE, which could result from different combinations of failures, are initially considered. Then, a screening process is applied to eliminate only very unlikely sequences.

4.2.2. Dynamic event trees in E-BEPU.

When a plant transient is triggered by an initiating event, the evolution of the plant state leads to crossing one or more set-points for safety system initiation. This occurs, in accordance with the plant protection design, when some safety function is required to reorient the plant state evolution towards a safer state. In some cases, the required safety function consists of disconnecting (tripping) some systems from the plant process in order to prevent their potentially harmful effects. In other cases, the safety function is performed by emergency equipment, usually in stand-by, which is connected to the process in order to mitigate the effects of the ongoing transient.

In both cases, i.e., a connection or disconnection event, the result of the safety system intervention is a change in the plant systems configuration. However, the actuation of the safety system is not failure free and the resulting configuration is not pre-determined. There could be different reasons for a safety system to fail. In disconnection events, for example, a breaker could fail to open or an isolation valve could fail to close. In connection events, a pump could fail to start-up or an injection valve could fail to open. Among the possible resulting configurations, some of them could be able to accomplish the required safety function and others will be inefficient.

In applying the E-BEPU methodology, whenever a safety system set-point is reached, the possible resulting configurations must be identified but no assumption is done about the ability of each configuration to achieve the intended safety function. Being E-BEPU a simulation based methodology, the plant state evolution and its safety characterization are not assumed but calculated. Therefore, when the simulation identifies that a safety set-point has been reached, the simulation process is split into several branches in order to continue the simulation with each possible configuration. New set-points can be reached in each branch, giving rise to new branching points. The resulting simulation structure is an event tree where the plant dynamics is calculated in detail. This type of event tree is known as dynamic event tree.

A dynamic event tree in E-BEPU has many similarities with a PSA event tree. The event tree headers represent demanded safety functions and when this demand occurs in a given sequence, a branching point appears below the corresponding header. There are, however, some differences that should be pointed out. The most evident one is that branching points in PSA fault trees are always binary, i.e., only two branches start at every branching point, while dynamic E-BEPU event trees may contain branching points with multiple output branches. This is so because safety functions in PSA and E-BEPU event trees are not represented in the same way. In PSA, safety functions are modelled in terms of success or failure and, therefore, there are only two possible results. In E-BEPU, safety function performance depends on the actual safety system configuration and, in a general case, there could be several possibilities.

Event tree headers, both in PSA and E-BEPU, are modelled with fault trees. A fault tree is a logical structure representing how system or safety function failures depend on the occurrence of basic events, usually defined at the level of elemental components. Knowing the probabilities of the basic events and the structure of the fault tree allows for calculating the probability of the final event (called top event) of the fault tree.

A fault tree with a single top event is enough to model a PSA header. Such top event is the failure of the safety function and success is just its complement. The definition of success/failure for a safety function (success criterion in PSA terminology) results from generic studies that determine the minimum capabilities of the safety systems which are necessary to achieve the safety function goal. Among the possible configurations of the safety system, all those providing the minimum capability or a higher one are considered successful; the others are considered failed. Any failed configuration is assimilated to the total failure of the safety system (lower branch in the event tree) and all the successful

configurations are considered equivalent and assumed to provide the nominal performance of the safety function (upper branch of the event tree).

In dynamic event trees, however, a header representing a safety system with n possible configurations should be modelled with fault trees ending in n-1 top events, with the last configuration being the complement of the others. Each top event corresponds to a particular output branch of the branching point. E-BEPU fault trees are therefore different from PSA fault trees but, since PSA success criteria strongly depend on configurations, PSA fault trees do contain information about configurations. It depends very much on the modelling technique followed in PSA how easy is to extract configuration fault trees from PSA fault trees. Whenever feasible, this possibility should be used. Developing new fault trees for E-BEPU is a huge effort that, to a great extent, would repeat the effort already devoted to the development of PSA.

There are cases where the number of configurations could be really high. Let us consider, for example, a safety injection system of a PWR composed by three trains, with two flow paths (i.e., injection to hot or cold legs) and three injection points per flow path, one for each primary coolant loop. The combination of number of active trains, number of flow paths and number of effective (i.e., open) injection points results in a number of configurations that could result prohibitive, especially taking into account that those configurations may need to be combined with the configurations of other safety systems. When the resulting number of configurations is significantly high, it is acceptable, even advisable, to reduce the number of analysis cases by grouping or bounding configurations using adequate criteria.

Grouping configurations is a suitable technique when several configurations are expected to produce similar effects on the plant processes. For example, in a three train system, actuation of any combination of two trains will likely produce equivalent effects. In such cases, all the equivalent configurations can be grouped and only one of them is simulated.

Bounding configurations consist of replacing a set of non-equivalent configurations by a single one producing the most unfavorable results. For example, if a qualitative analysis shows that several configurations have little chance of achieving the safety function goals, it could be acceptable to simulate only the one producing the worst results and assign the same results to the other configurations. It is also possible to bound several sequences with high chance of success with a single one where success is achieved with the lowest margin.

It should be noted that PSA headers can be seen as the result of applying bounding techniques to the point of keeping only two final configurations, one for safety function success and the other for safety function failure. The success configuration is the one defined as the header success criterion, i.e., representing the minimum capabilities to get success. The failure configuration is the total lack of intervention of the safety system.

4.2.3. Sequence identification

Taking into account the above discussion, identification of sequences starting from a PIE is a simulation result. Safety systems only come into play if they receive a demand signal and, when simulating the plant state evolution following the occurrence of the PIE, the condition that some safety system set-point has been reached can be easily identified. At that point, the safety system will change the course of the plant state evolution (unless a total failure occurs) with effects that depend on its effective configuration.

For each possible configuration, the subsequent evolution of the plant state shall be simulated and new set-points could be reached before getting either a stable safe state, a failed state where some acceptance criterion has been exceeded or the completion of a pre-established mission time for the analysis. For each new set-point, this process is recursively applied and the whole dynamic event tree gets identified.

It is important to highlight the importance of set-points in the process of sequence identification. Opening a branching point for safety system intervention only makes sense if a demand set-point has been reached. Actually, one of the objectives of the analysis of design basis events is to verify the correctness of set-points. Note that a set-point that is not well designed and/or calibrated, can result in lack of effectiveness of the safety function or in undesired effects because of untimely intervention. Revising safety system set-points will be one of the priority actions in case of unsatisfactory results of the analysis of a PIE.

Another aspect that reflects the importance of correct set-point activation is the very different safety significance that the lack of intervention of a required safety system may have depending on the reason for remaining inactive. If a set-point is reached, the corresponding demand signal is issued but the system does not actuate, we can ensure that the system has failed. However, if the system set-point is incorrect and the system actuation is not demanded when necessary, we should not assume that the system has failed. In both cases, the dynamic evolution of the plant state will be the same because no safety function is being implemented but the probabilistic characterization of the two cases is radically different.

The total failure of a demanded safety system is, in event tree terminology, one of the output branches of a branching point. Hopefully, this branch would be of very low probability since safety systems are expected to be very reliable. Consequently, the sequence where this branch is included will likely be of low importance in the analysis of the whole PIE. It could even happen that this sequence would result screened out according to the criteria that will be explained later.

On the contrary, lack of intervention due to an incorrectly designed set-point is not related with any branching point in the event tree and no low probability factor is lowering the sequence probability. The predictable exceedance of acceptance criteria under these conditions will have a significant weight in the analysis of the PIE and will likely contribute to unacceptable analysis results.

In the design process, determining the optimum set-point of a safety system can be the result of a sensitivity analysis. In the verification process, which is the objective of E-BEPU, the possibility of a set-point drift may be included in the uncertainty analysis if convenient.

4.2.4. Sequence quantification

Identifying the sequences of the dynamic event tree implies that the fault trees involved in each sequence are also identified. The quantification process to determine the sequence probability, conditional to the occurrence of the PIE, is similar to PSA case. From the point of view of fault trees, a sequence is the combined event that results from considering that all the events involved in the sequence have occurred. Since each of these events has an associated fault tree, the AND combination of all these fault trees can be defined as the sequence fault tree.

Fault trees are Boolean functions describing which combinations of basic events result in the occurrence of the top event. The AND combination of these functions consists of calculating their Boolean product. This is a simple operation when there is independence between the fault trees being combined but, unfortunately, this is not the case of PSA fault trees, nor of E-BEPU fault trees. In most cases, there are common basic events in the component fault trees and the product of the Boolean functions becomes a more complex operation.

This also complicates the quantification process. Quantification consists of propagating the probabilities of basic events through the fault tree structure, i.e., through the Boolean function, to obtain the probability of the top event. In the hypothetical case of independent fault trees, the probabilities of the top events composing a sequence could be calculated from their corresponding fault trees, independently of each other, and the sequence probability would be the arithmetic product of the probabilities of the component top events. The real case is much more complex since the quantification of the sequence probability

cannot start until all the component fault trees have been identified and their Boolean product has been calculated.

Let us consider again the hypothetical case of independent fault trees. In this case, each time the simulation identifies a branching point and a particular output branch is followed, its corresponding fault tree could be quantified and the resulting probability, multiplied by the probabilities of previous events in the sequence, would be the probability of the occurred part of the sequence. In other words, the calculation of the sequence probability would be a cumulative process where previous results are used in the calculation of the next step.

In the real case of non-independent fault trees, the cumulative calculation of the sequence probability is not possible or, at least, not easy. Of course, at any moment in the sequence evolution, it is possible to calculate the probability of the occurred part of the sequence by performing the Boolean product of the events occurred so far and then to quantify the joint probability of those events. However, if a new event is later added to the sequence, the previous calculation is useless and the quantification of the extended sequence must be initiated from scratch.

The computing power needed to perform Boolean products and probability quantifications depends on the format of the Boolean functions and the quantification algorithm. Most PSA quantification codes use the *cut set* format because it provides very useful information about the relationship between basic events and top events. However, for quantification purposes, the *cut set* format is far from optimal because it is slow and its accuracy is always limited by the need to truncate some terms of the probability calculation. As a result, quantifying the sequence probability whenever a new event appears is often a very expensive operation in terms of computing power and, in many cases, it may result prohibitive.

4.2.5. Sequence screening

As explained later in Section 4.3.3, the uncertainty analysis of a PIE, which is the essence of E-BEPU, is obtained on the basis of the uncertainty analysis of the individual sequences starting from the PIE. Sequences with high conditional probability contribute very much to the characterization of the PIE uncertainty while low probability sequences may give a very low, even negligible contribution. Devoting a significant effort to simulate sequences with very low contribution to the results of the analysis does not make much sense. Because of that, it is advisable to establish a minimum conditional probability value below which a sequence can be left out of the uncertainty analysis and, therefore, out of the analysis of the PIE. This probability value will be referred to as P_{cutoff}. Section 4.3.3 also provides some criteria that help determining the value of P_{cutoff}. Typically, this value will be lower than 5E-4.

It must be emphasized that sequence screening is different from determining the boundaries of the design basis. When describing accident classes in 4.1 it was mentioned that accidents with frequency lower than an exclusion frequency could be left out of the design basis. The exclusion frequency and the cut-off probability are not related in any way. Moreover, the exclusion frequency filter is applied before starting the E-BEPU analysis while P_{cutoff} is applied at individual PIE level in the analysis stage.

Sequence screening is mainly done on the basis of a probabilistic criterion. However, E-BEPU establishes as a cautionary measure for ensuring an adequate level of Defence-in-Depth, that sequences involving a single failure (additional to the PIE) cannot be screened out. Quantifying all the possible sequences before applying the screening criterion and identifying the single failure sequences requires simulating the whole dynamic event tree in order to verify the correctness of the sequences. Therefore, the simulation of very low probability sequences cannot be totally avoided but, at least, it can be reduced to a minimum. Note that the identification of a sequence and, therefore, its quantification, can be based on a single simulation but the sequence uncertainty analysis requires a significant number of simulations.

There is another precaution that must be taken during the sequence screening process. Not only must the conditional probability of an eliminated sequence be lower than P_{cutoff}. Additionally, it must be verified that the collective importance of all the sequences that have been screened out is low enough. To this purpose, the same P_{cutoff} criterion can be applied and, therefore it is also required that the joint conditional probability of all the sequences that have been excluded is lower than P_{cutoff}. The purpose of this precaution is preventing that an abusive introduction of event tree headers or an unjustified number of output branches in branching points could lead to the elimination of an unacceptable number of sequences.

In summary, the screening process can be applied as follows:

1. It is assumed that an adequate simulation model is available for the analysis of the PIE and that a set of significant uncertain parameters have been identified.

2. A simulation is started from the PIE using any set of uncertain parameter values. If a simple random sample of those parameters has been already obtained (see 4.3), the first set of values in that sample can be used.

3. With those parameter values, the dynamic event tree is developed and all the possible sequences get identified.

4. The conditional probability of each identified sequence is calculated from the corresponding fault trees.

5. Sequences with conditional probability lower than P_{cutoff} are provisionally screened out, except in the case of sequences containing a single failure, which are kept in the analysis scope.

6. The joint probability of all the excluded sequences is evaluated. If it is lower than P_{cutoff}, the exclusion of those sequences is confirmed. Otherwise, some of the provisionally excluded sequences must be recovered for the analysis.

7. For all the sequences that have not been screened out, the uncertainty analysis continues by running all the required simulation cases (see 4.3).

4.2.6. Additional considerations for manual actions

Design basis analysis mainly deal with the behavior of automatic protections. The uncertainties that are usually considered both in BEPU and E-BEPU are related with parameters of the simulation models or with initial and boundary conditions of the simulation.

There are, however, some cases where the analysis of a PIE includes some specific manual action that is necessary to comply with the applicable acceptance criteria. The traditional approach in these cases is to assume in the simulations that the action is executed with a fixed delay with respect to the moment when it becomes necessary. If the action is demonstrated efficient when executed with this delay, it is also assumed that an earlier execution is equally efficient but, if executed later, its efficiency is not ensured and the safety function it tries to implement should be considered failed.

A more realistic analysis approach would be to consider that the execution delay of the action is an additional uncertain element of the analysis. However, if time uncertainty is incorporated into the analysis, some precautions are necessary. It should be noted that delaying a protective action may have a significant impact in the subsequent plant state evolution. Indeed, this time uncertainty may be dominant over other parametric uncertainties and it could even involve changes in the sequence itself if an excessive delay allows for the arrival of a new event before the action becomes executed. Should this occur, the delay

probability distribution would be used for two different purposes. On the one hand, the new sequence must be incorporated to the dynamic event tree with a new output branch from the branching point of the manual action and the corresponding probability must be assigned to this branch. On the other, the delay time must be sampled in all the output branches in a consistent way.

Introducing uncertain time delays in an E-BEPU analysis is a complex issue. Identifying possible sequence changes may require performing first a sensitivity analysis. The implications that this type of sequence change may have in the BEPU sampling process have not been analyzed yet. It is therefore recommendable not to include time delays in the uncertainty analysis if the possibility of sequence changes due to large delay values cannot be excluded.

4.3 Sequence and PIE uncertainty analysis (Blocks 3 to 10).

In Block 2 of Figure 4.1, the possible sequences starting from the initiating event, with or without additional failures, are obtained. The conditional probability of each sequence is calculated, and sequences with a probability higher than P_{cutoff} are kept. All single-failure sequences are retained even if they have low probability (required by DiD). In the following, any reference to "all the sequences derived from the PIE" should be interpreted as "all the sequences derived from the PIE that have not been screened-out".

In this section it is described how the uncertainty analysis is performed in the E-BEPU methodology. The reader should be warned that some of the actions and questions of the blocks described in this section apply to the whole set of sequences derived from the PIE while others refer to individual sequences. The applicability scope of each block will be a part of this description.

In Block 3, a BEPU analysis (i.e., similar to Option 3 DSA) is performed for each sequence retained from those deriving from the PIE.

There are different possible approaches to the BEPU analysis. A first criterion distinguishes between input-driven and output-driven. Essentially, the former approach estimates the uncertainty of the input parameters and propagates it through the calculation (i.e. through the code) to the safety outputs, also called Figures Of Merit (FOM). The second approach estimates the accuracy of the safety outputs by comparing code predictions and real values for experimental tests, and then extrapolating the accuracy to a full scale nuclear plant.

Another criterion distinguishes black-box from white-box approaches, the former being an approach which does not benefit from the knowledge of the predictive model (code). White-box approach, on the other hand, uses the knowledge of models and correlations within the code to optimize the uncertainty analysis.

The present Option 4 methodology is valid whatever the type of BEPU method is used in the sequences analysis. Anyway, we will give a special relevance to the most widely used BEPU methodology. It is a black-box, input-driven and probabilistic approach based on the well-known Wilks' method [Wilks, 1948]. This approach is illustrated in Figure 4.5. Assuming that a single, scalar safety output is calculated (having an upper regulatory limit), it is assumed that the BEPU analysis has the following stages:

1. The input parameters that most influence the safety output are identified, and probability distributions (representing their uncertainty) are assigned to them. It is important to ensure that input uncertainties are not underestimated.
2. Uncertain inputs are sampled from their distributions, so that a simple random sample (SRS) of the inputs is obtained. The sample size is predetermined, and typically is obtained from Wilks' formula [Wilks, 1941] that implements the same principle of pure Monte Carlo propagation.

3. The code is run for the SRS of input decks, thus producing a SRS of the safety output with the predetermined sample size.
4. A tolerance limit, with the regulatory tolerance level, is obtained for the safety outputs. It is obtained with Wilks' nonparametric method. Such limit is compared with the regulatory acceptance limit.

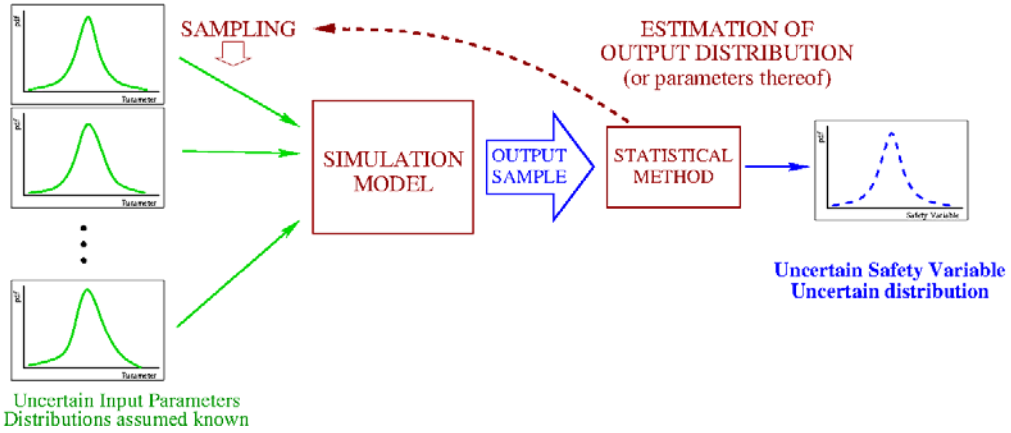

Figure 4.5: Black-box, input driven, probabilistic approach for uncertainty propagation.

Inputs to a BEPU analysis include:

- Initial and boundary conditions
- Material properties
- Model parameters i.e. quantities included in the formulation of models and correlations of the code
- Geometrical parameters
- Plant operational parameters
- …

For the performance of a BEPU analysis, a great deal of effort must be devoted to assigning probability distributions to the uncertain inputs. As indicated before, a basic principle is that the assigned uncertainties must not be underestimated, at least in the "conservative direction" (i.e., the most unfavorable values) of the parameter.

An important class of inputs are the operational parameters which are controlled by the Technical Specifications (TS) of the plant. It is important to remind that a safety analysis must prove that the allowed operation of the plant (i.e. the operation within TS limits) is safe, rather than proving only that the "normal" operation of the plant is safe. For this reason, the probability distributions assigned to operational parameters must "explore" the operational regions around the TS limits, rather than the "normal operation" regions [19].

Tolerance limits are statistical artefacts, which we next define. Suppose that X is a scalar random variable with a continuous cumulative distribution function (CDF), and $X_1,\ldots, X_N$ is a SRS of X. An upper tolerance limit of X, with tolerance level (P, C), is an upper confidence limit (with confidence level C) of the quantile of order P of X. Such confidence limit is obtained from the SRS of X. P and C are real numbers in the interval (0, 1). P is called the probability or coverage level, and C is called the confidence level.

In other words, an upper tolerance limit of X is a quantity calculated from a random sample and having the property of bounding the P-quantile of X with confidence of at least C.

Similarly, a lower tolerance limit is a lower confidence level of a quantile of X.

Tolerance limits are *statistics*, meaning that they are functions of the random sample. If we discard our SRS and obtain a new one (with the same size), the tolerance limit calculated from the two samples are (in general) different.

4.3.1. Wilks' method

Wilks' method uses order statistics as tolerance limits [20][21]. Given a simple random sample (with size N) of a scalar random variable X, the corresponding ordered sample is simply obtained by sorting the sample elements from the lowest to the highest. The order statistics of ordinal r ($r \leq N$) is the r-th element in the ordered sample, represented by $X_{r:n}$. Therefore, $X_{1:N}$ is the sample minimum and $X_{N:N}$ is the sample maximum.

Wilks proved that, if some conditions are fulfilled, the order statistics $X_{r:n}$ is an upper tolerance limit of level (P, C) of X. Such conditions are defined in an equation which is called the one-sided Wilks' formula, and it relates the tolerance level (P, C) to the sample size N and the ordinal r. Given P, C and r (this last as a function of N), there is a minimum sample size N_{min} solving one-sided Wilks' formula. For instance, well-known results are:

- For P = C = 0.95 and r = N, N_{min} = 59. This means that the maximum of a sample of 59 is a (95, 95) upper tolerance limit.
- For P = C = 0.95 and r = N-1, N_{min} = 93. This means that the second maximum of a sample of 93 is a (95, 95) upper tolerance limit.
- For P = C = 0.95 and r = N-2, N_{min} = 124. This means that the third maximum of a sample of 124 is a (95, 95) upper tolerance limit.

N_{min} is the minimum size of the SRS needed to perform the uncertainty analysis. It is important to remember that each of the elements of the sample involves a run of the code, which transforms the input into the output. Thus, N_{min} is a measure of the computational effort needed for the uncertainty propagation.

Up to now, our discussion has focused on the calculation of an upper tolerance limit. A similar method is followed for obtaining a lower tolerance limit via Wilks' theory. In fact, a simple change of sign of the random variable transforms lower limits to upper limits and vice versa.

The standard value of the tolerance level established by regulators for BEPU analysis in Deterministic Safety Analysis is (95, 95). In the following we will term it the *standard tolerance level* STL.

As we have stated, analyzing an accident sequence at the (95, 95) level means that we estimate (with at least 95% confidence) the 0.95-quantile of the safety output, and compare it with the regulatory limit L. The fulfilment of the RAC can be statistically stated in two different but equivalent forms:

- The 0.95-quantile (i.e. the 95 percentile) of the safety output is lower than L with (at least) 95% confidence.
- The probability that the safety output exceeds L is lower than 0.05 with (at least) 95% confidence.

4.3.2. Tolerance limits in E-BEPU.

When applying the Wilks' method for E-BEPU, it is easily proved [22] that, if all the analysed sequences fulfil the RAC with the STL, the PIE as a whole also fulfils those criteria with the STL. For this reason, a positive answer to the question in Block 4 (*Do all sequences fulfil acceptance criteria with STL?*) implies that an explicit evaluation of the whole PIE is not necessary. On the contrary, if one or more sequences fail compliance with the applicable acceptance criteria with STL, the analysis flow is directed to Block 8 which will be discussed

later. From now on, sequences fulfilling the RAC with STL will be referred to as “successful sequences” while the remaining will be called “failed sequences”.

But, even if all the sequences derived from the PIE are successful, the work is not completed, because further requirements are needed to minimize the so-called cliff-edge effects, which are unacceptable in the context of IAEA SF-1.

According to *IAEA Safety Glossary*, a cliff-edge effect is a “severely abnormal plant behavior caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input”. The existence of cliff-edge effects will produce, in general, an increase of the probability that safety outputs surpassing their acceptance limits could reach values involving a level of severity much higher than the one represented by those acceptance limits.

In order to prevent cliff-edge effects, it is necessary to impose new requirements on the safety outputs, so that some percentile orders higher than 95 are subject to regulatory limitation. This is a new requirement in E-BEPU, represented by Block 6 of Figure 4.1.

We define the *increased tolerance level* (ITL) as (99, 95), meaning the construction of a tolerance limit covering the 99^{th}-percentile of the FOM with 95% confidence. The solution of one-sided Wilks’ formula for P = 0.99, C = 0.95 produces the following results:

- For r = N, N_{min} = 299. This means that the maximum of a sample of 299 is a (99, 95) upper tolerance limit.
- For r = N-1, N_{min} = 473. This means that the second maximum of a sample of 473 is a (99, 95) upper tolerance limit.
- For r = N-2, N_{min} = 628. This means that the third maximum of a sample of 628 is a (99, 95) upper tolerance limit.

It is evident a significant increase (approximately by a factor 5) on the minimum sample size needed in the construction of the new tolerance limit. This increase makes sense, because the minimum sample size should be a growing function of the percentile order to be covered.

In the E-BEPU methodology, apart from fulfilling the RAC of the PIE class with the STL, it is required that each sequence fulfils the RAC of the next class of accidents with the ITL (Block 6). In other words, a less strict criterion is additionally required, but with a stricter tolerance level. In Block 5, the next class RAC are identified. Note that this requirement applies to individual sequences that were initially considered successful. Failure of a single sequence to comply with this new requirement would lead to output “no” of Block 6 and, therefore, to considering the design inacceptable.

This double requirement for acceptance of successful sequences is qualitatively illustrated in Figure 4.6 where the 0.95 and 0.99 quantiles are compared with the acceptance criteria of the PIE class and the next class, respectively.

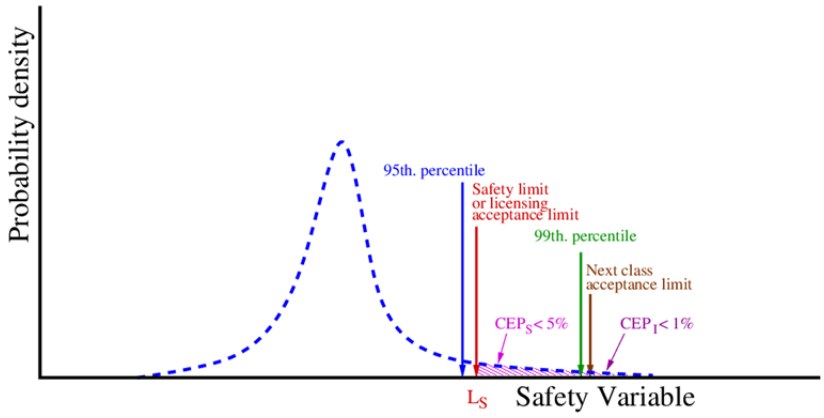

Figure 4.6: The double requirement for acceptable success sequences in E-BEPU

As an example, let us consider a sequence derived from a PIE of moderate frequency, with an acceptance criterion requiring the fraction of fuel rods in critical heat flux condition (FCHF) to be below a limit (e.g. 0.001). For the next category (infrequent events), the acceptance criterion is less strict (with a higher limit for FCHF e.g. 0.1). In E-BEPU, the first criterion is required with the STL, while the second is required with the ITL.

For sequences starting from a PIE of the last class, the requirement to fulfil the next class criteria with ITL is, in general, not applicable because there is no “next class”. Therefore, Blocks 5 and 6 are bypassed for sequences of the last class (this bypass is not represented in Figure 4.1) and the analysis flow reaches Block 7 (Design is acceptable). This does not mean that cliff-edge effects are not adequately prevented in these sequences. Note that exceeding the limits of the last class leads to the field of PSA where additional systems and/or operator actions are considered in order to prevent escalation to a severe accident. How effective is this prevention, however, is beyond the scope of E-BEPU.

4.3.3. Uncertainty analysis of the PIE.

It could happen that when performing the sequence uncertainty analysis of Block 3, one or more sequences result failed, i.e., not fulfilling the RAC for the class of the PIE at the STL. In this case, an uncertainty analysis of the PIE must be explicitly performed (Block 8) to ensure that the PIE “as a whole” satisfies the RAC with STL (Block 9).

We have described how to make a BEPU analysis of each sequence derived from a PIE. The procedure follows the “Option 3” assumptions; the uncertainty is propagated from the inputs (including initial and boundary conditions) and from physical models of the code, but the configuration and performance of safety systems is postulated in each sequence.

Then, what do we mean by the uncertainty analysis of a PIE? Firstly, it is interesting to define the outcome of the PIE as a “combination” of the individual sequence outcomes. Given a PIE, there are a set of sequences developing from it. Let us call R the total number of sequences retained after sequence screening (Block 2), each sequence being identified as S_i with i varying from 1 to R. Each sequence is characterized by its conditional probability π_i, calculated also in Block 2. It is clear that we can invert this statement and define the PIE as the event that follows each sequence S_i with probability π_i. In the probability theory jargon, it is said that the PIE is a “finite mixture” of the sequences derived from it.

Suppose a calculated safety output (i.e., a FOM) Y for the PIE. Then, Y can be defined as the finite mixture of the Y_i with probabilities π_i, i = 1…R.

Let us remind that the sequences have been previously analysed one by one via a pure Monte Carlo analysis with a predetermined sample size (fulfilling Wilks’ formula with the

STL). Therefore, there is available a simple random sample of each safety output Y_i, i = 1…R. Let SRS_i be the SRS of Y_i.

It is possible to construct, from this collection of SRS, a simple random sample for the PIE, using the following procedure: select randomly a sequence according to the conditional probabilities π_i, and then choose randomly an element from the SRS of the selected sequence. The chosen element is suppressed, and the operation is repeated until the SRS of desired size is obtained.

Typically, there is one sequence (the one without failures) much more probable than the remainder. For small sample sizes (recall that the smallest size of the STL is 59), there is a high probability that all the sample elements for the PIE are extracted from the SRS of this dominant sequence. For the same reason, it is very unlikely that sequences with very low probability may contribute the SRS of the PIE.

As an example, suppose that a PIE produces two sequences: S_A with probability 0.999 and S_B with probability 0.001. We want to construct a SRS of size 59 for the PIE from the two SRS of size 59 of the respective sequences. The probability that we select all the 59 elements from S_A (i.e. no element from sequence S_B) is 0.999^59 = 0.943

Should this be the case, the BEPU analysis of the PIE may be easily reduced to the BEPU analysis of the dominant sequence at the cost of introducing some non-quantified error in the PIE analysis.

Another procedure to check the fulfilment of acceptance of acceptance criteria for a PIE in a sequence-by-sequence fashion is based on the analysis of a partial subset of the sequences derived from the PIE. In [22] and [23] it is proved that the BEPU analysis of the PIE can be focused on a group of dominant sequences accumulating at least P probability (where P is the regulatory coverage level) and therefore discarding the remaining set of sequences with an accumulated conditional probability π_{disc} lower than 1-P. Then, a sufficient condition for the PIE fulfilling the RAC to a level (P, C) is the fulfilment of the RAC in every dominant sequence to an "augmented" tolerance level (P*, C), where the new coverage level P* is equal to P divided by (1-π_{disc}).

Recall the previous example, with sequences S_A (prob. 0.999) and S_B (prob 0.001). Then, to prove that the PIE satisfies the RAC to (95, 95) level, it is sufficient to ignore S_B and prove that the sequence SA satisfies the RAC to an augmented tolerance level (P*, 95), where P* is 0.95 divided by 0.999, i.e., 0.951. As previously stated, the minimum sample size obtained from one-sided Wilks' formula is increased when the coverage level is augmented. In our example, the minimum sample size for a sample maximum and tolerance level (95.1, 95) is 60. So, the augmented coverage level produces a minimal increase in the sample size (from 59 to 60).

If the discarded sequences amount a very small probability, the Wilks' minimum sample size will remain unchanged. For instance, if the discarded probability is less than 5E-4, the minimum sample size for sample maximum remains 59. This gives a solid argument to determine an adequate value for P_{cutoff} in Block 2. Note that a value of π_{disc} fulfilling this condition is also a very adequate value for P_{cutoff}. Therefore, if the maximum of a sample of size 59 is being used for checking the STL, it is recommendable to use 5E-4 as an initial value for P_{cutoff} that can be further refined with other criteria, if necessary.

If the analysis of Block 8 shows that the PIE does not fulfil the acceptance criteria with the STL, the exit from Block 9 would follow the "no" output. This means that the design in not acceptable.

If the PIE analysis is successful, the analysis flow reaches Block 10 where failed and successful sequences are separated in such a way that successful sequences are redirected to Blocks 5 and 6 where compliance with next class RAC is required at ITL. Failed

sequences, on the contrary, are forwarded to Block 11 where sequence reclassification is considered as described in next section.

4.4 Sequence reclassification (Blocks 11 to 13).

Reaching Block 11 of the flow diagram of Figure 4.1 means that in the BEPU analysis of Block 3 there were some failed sequences that, nevertheless, did not accumulate enough probability as to make the PIE analysis of Block 8 unsuccessful. Then, the sequences were filtered in Block 10 and only the failed sequences reach Block 11. The analysis described in this section shall be applied to each failed sequence, one by one.

A failed sequence does not fulfil the acceptance criteria of the PIE class with STL and its conditional probability is too high to be screened out. However, if this probability is low enough, E-BEPU allows for moving the sequence to the next class were it is evaluated against the corresponding acceptance criteria. However, for reclassified sequences, the fulfilment of the acceptance criteria is required with the stricter ITL.

This feature of E-BEPU can also be stated in a different way as follows. Every sequence starting from the PIE that has not been screened out should, in principle, comply with two requirements, namely, to fulfil the RAC of the PIE class with STL and to fulfil the next class criteria with ITL. The second requirement can never be eluded. A single sequence that does not meet the second requirement leads to concluding that the design is not acceptable (Block 15). However, the first requirement could not apply if the sequence has a low enough probability. The question is then, what is a low enough probability? The key word to answer this question is reclassification.

Figure 4.7 represents a section of the class limits of Figure 4.4 for two consecutive classes. Let i be the class to which the PIE belongs and i+1 the next one. In the usual logarithmic scale used for frequencies in typical risk graphs, the graphic distance between the two frequency limits is given by the quotient F_i/F_{i+1}. The inverse of this quotient is a non-dimensional number, lower than 1, which can be interpreted as a probability. We are trying to justify that this number can be properly used as reclassification criterion in E-BEPU and therefore it can be called $P_{reclassify}$.

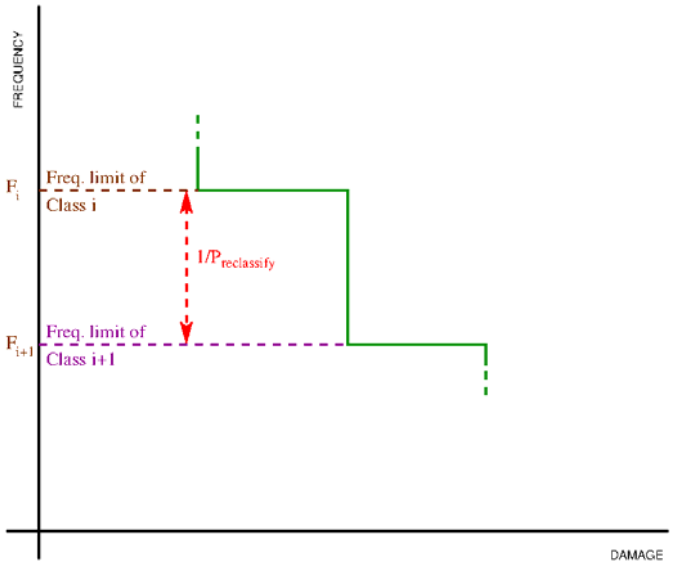

Figure 4.7: The sequence reclassification criterion in E-BEPU

If the frequency of the PIE would be known with some precision, it would be possible to calculate the frequency of any sequence with a comparable precision by multiplying the former by the conditional probability of the sequence. Then, from the calculated sequence frequency, it would be possible to estimate if its frequency is low enough as to consider this sequence an acceptable contributor to the next class frequency.

Let us recall that, according to Figure 4.4 and the discussion in section 4.1.1, an accident class is defined by a damage limit and a frequency limit. The frequency limit is the maximum allowed accumulated frequency of all the accidents belonging to the class. It was stated in section 4.1.1 that frequencies of individual accidents matter only as contributors to the accumulated frequency of the class.

Any sequence starting from a PIE is a contributor to the PIE frequency and, therefore, to the frequency of its class. In most cases, the PIE frequency is not accurately calculated but, if it has been adequately classified, the PIE itself and all the sequences started from it are considered acceptable contributors to the frequency of its class. An acceptable contributor is such that its frequency is low enough with respect to the class frequency limit that, even when it is summed up with other contributors, the limit is not reached. In addition, it should be recalled that the frequency of a sequence is the frequency of the PIE (whatever it is) multiplied by the conditional probability of the sequence.

Reclassifying a sequence in E-BEPU means that this sequence is no longer considered to contribute to the PIE class frequency but to the next one. The reclassification will be allowed if the reclassified sequence is an acceptable contributor to the frequency of its new class.

Unfortunately, we do not know the frequency of the PIE. We only know (by assumption) that it is an acceptable contributor to the frequency of class i or, in other words, that its frequency is low enough with respect to the frequency limit F_i. If the conditional probability of a sequence is $P_{reclassify}$ or lower, it can be reasonably expected that its frequency will be low enough with respect to the frequency limit F_{i+1} and the sequence can be considered an acceptable contributor to the frequency of class i+1.

For a sequence starting from a PIE of the highest class, reclassification would mean moving the sequence to the Beyond Design Basis territory. Consequently, the reclassification would be allowed if the frequency of the sequence can be considered an acceptable contributor to the frequency of Beyond Design Basis scenarios. As described in 4.1, the frequency limit for these scenarios is the exclusion frequency of Figure 4.4 that we call now F_{ex}. Therefore, the reclassification criterion for sequences of the last class (say class N) will be $P_{reclassify} = F_{ex}/F_N$.

As in the case of non-failed sequences (Blocks 5 and 6, see 4.3.2), reclassified sequences coming from class N cannot be compared with any acceptance criterion of the new class and, therefore, Blocks 12 and 13 are bypassed and the analysis ends up in Block 14 (Design is acceptable). The difference with respect to successful sequences is that failed and reclassified sequences coming from a PIE of class N do not comply with the PIE class criteria at STL (they are failed) and they are not compared with other criteria because they do not exist. Thus, they are *de facto* excluded from the analysis.

Being low frequency sequences that did not prevent compliance of the whole PIE with the applicable criteria, this exclusion can be, in general, accepted. The only questionable case would refer to single failure sequences which, in the screening process of Block 2, are never eliminated in order to maintain an adequate level of Defence-in-Depth. However, when a sequence of class N is reclassified, it is moved to a beyond design category (also called design extension category in recent standards). Standards for the analysis of accidents in these categories do not usually require the application of the single failure criterion and, therefore, the exclusion of sequences with a single failure would be acceptable.

In summary, the process described by Blocks 11 to 13 of Figure 4.1, which is applicable to every failed sequence, is as follows:

1. Determine the frequency limits of the PIE class (F_i) and the next class (F_{i+1}). Calculate $P_{reclassify} = F_{i+1}/F_i$; ($P_{reclassify} = F_{ex}/F_N$ for last class sequences).
2. If the conditional probability of the sequence, calculated in Block 2, is higher than $P_{reclassify}$, leave Block 11 through the "no" exit leading to the conclusion that the design is unacceptable (Block 15).
3. If the sequence can be reclassified, go to Blocks 12 and 13. These blocks are identical to Blocks 5 and 6. The difference is that Blocks 5 and 6 apply to successful sequences while Blocks 12 and 13 apply to failed (and reclassified) sequences.

If all the failed sequences filtered in Block 10 reach the "yes" exit of Block 13, the design will be considered acceptable. If any of these sequences goes through the "no" exits of Block 11 or Block 13, the design should be reconsidered.

4.5. Design unacceptability and remedial actions (Block 15)

The design of a safety system is based on one or several initiating events demanding its action to comply with the associated safety function and acceptance criteria e.g.: a PWR large break LOCA is the design event for low pressure injection system under the assumption of system single failure and previous (N-1) accumulators effective discharge. The correctness of the design should be assessed with suitable analysis methodologies among which E-BEPU is a possible choice.

In order to verify the completeness of the assessment a series of requisites should be fulfilled in the application of E-BEPU:

- For a given postulated initiating event (PIE) all sequences requiring the action of safety systems have to be identified and assessed up to the truncation probability. Only sequences whose probability P_{seq} is low enough, i.e., $P_{seq} < P_{cutoff}$, can be discarded, provided that the cumulative probability of all the discarded sequences is still low enough.

- The assessment of scenarios assuming single failure on safety systems shall never be excluded based on probability arguments. The single failure criterion requirement contributes to assure compliance with defence in depth criteria[4].
- For a given PIE, compliance with acceptance criteria of the class to which the PIE belongs with the STL (typically, 95/95) is required. For anyone of the non-discarded sequences this condition is also required unless the sequence can be reclassified. In order to limit a potential cliff edge, sequences are also required to fulfill the acceptance criteria of next class with an Increased Tolerance Level (ITL), e.g., 99/95.

4.5.1 General approach to the analysis of design deficiencies in E-BEPU

As a result of the analysis of a given PIE, several deficiencies can be observed that lead to reaching Block 15 in the E-BEPU flow diagram (Figure 4.1).

a) Compliance of the PIE as a whole with the acceptance criteria is below the STL. This deficiency is represented by the "no" exit of Block 9 in the flow diagram.

b) The probability of one or more failed sequences, i.e., sequences not complying with the acceptance criteria of the PIE class at STL, is higher than the sequence

[4] Initial and boundary conditions transposed to Technical Specifications limiting conditions for operation should in any case be compliant with the single failure criterion.

reclassification threshold $P_{reclassify}$. That is, the acceptability of the sequence cannot be supported by compliance with the next class acceptance criteria. This corresponds to the “no” exit of Block 11.

c) One or more reclassified sequences fail to fulfil the acceptance criteria of the next class at Increased Tolerance Level (ITL). This is the case of the “no” exit of Block 13.

d) One or more sequences fulfilling the acceptance criteria of the PIE class at STL fail compliance with next class acceptance criteria at ITL. That is, an initially acceptable sequence may be prone to a cliff-edge effect. The “no” exit of Block 6 represents this deficiency.

In order to correct these deficiencies there is a need for a revision of the design. It can be observed that these deficiencies point to the need of increasing the success probability of the sequences associated to the PIE. This can be achieved by:

i. Enhancing the performance of safety systems (protection performance). In many cases, lack of performance could be due to inadequate initiation setpoints. In other cases, a better performance can be achieved by increasing the capacity of some system components, e.g., an injection pump.

ii. Enhancing the reliability of the safety systems (protection reliability). This way, sequences with protection failures could have a lower probability and become candidates for reclassification or elimination.

iii. Adding a new level of protection. That is, introducing a new safety system with its corresponding header in the dynamic event tree. This results in additional branching points in failed sequences. Examples could be an alternative rod insertion system, a dedicated diesel generator, etc. This way, sequences including the new protection would likely become compliant with the acceptance criteria while sequences where the new system is also failed would be of lower probability. Both effects would contribute to the acceptability of the PIE analysis results.

Solving a design deficiency with impact in one or several sequences may also be achieved by increasing the robustness of the affected safety barrier, in fact modifying the barrier safety limit. However, this goes beyond the E-BEPU methodology and will not be further discussed.

4.5.2. Enhancing performance

Assuming that physical models on the code and the applicable safety limits are adequately validated, design parameters affecting the safety system, plant initial conditions and safety system settings may be modified in order to improve the needed capability of the safety system to better cope with the effects of the PIE .

It is important to note that in many cases the poor performance of a safety system can be due to an incorrectly adjusted set-point. In such case, failed sequences could become successful if the activation set-points are modified. However, care should be taken to ensure that a set-point modification that could be convenient for a given PIE does not have negative effects for other PIE of for some operational states. Unneeded actuation of a safety system is undesirable even for safety reasons and the modification of its actuation set-point cannot be done on the basis of the analysis of a single PIE. Any PIE or operational plant state where the safety system could be involved must be analyzed before implementing a set-point modification.

Modifying the capability of safety systems requires identifying design parameters relevant to the compliance with the acceptance criteria at STL or ITL. To this aim it would be convenient to study the output sensitivity in order to promote compliance with the acceptance criteria. Unless the sensitivity is clearly dominant on one specific and easily accessible design parameter, it becomes convenient to perform an importance analysis of one at a time and

joint parameters (at least duplets) e.g.: accumulators discharge pressure and gas and liquid volume.

Once the importance analysis is completed and the set of relevant design parameters and their combinations (at least at duplet level) are identified, it is possible to rank the different alternatives. However, before deciding a particular option, it is also important to avoid or minimize potential negative impact on other sequences of the same or a different PIE. The final decision on the design change would be mainly based on the set of failed runs but the total verification of the adequacy of the change would require repeating the whole analysis of the PIE and possibly of other PIEs.

The main effect of enhancing protection performance would be to convert some failed runs (i.e., those where some limit is exceeded) into successful ones. This will have a beneficial effect, no matter the kind of deficiency that lead to unacceptable analysis results.

Increasing the number of successful runs has a direct effect on the compliance of PIE with class acceptance criteria at STL (Block 9).

Converting failed sequences that cannot be reclassified (Block 11) into successful ones eliminates the need of reclassifying them and contributes to compliance with the acceptance criteria of its class at STL. Those sequences are redirected to the “yes” exit of Block 10 and do not enter Block 11 anymore.

For the case of reclassified sequences failing next class criteria at ITL, the protection enhancement could either convert them into successful sequences that do not need to be reclassified (redirecting them to the “yes” exit of Block 10) or it could allow for compliance with acceptance criteria of the new class at ITL, moving them to the “yes” exit of block 13.

Finally, for the case of sequences complying with its class acceptance criteria at STL but failing next class acceptance criteria at ITL, the enhancement of protection performance will contribute to compliance with those limits with the effect of redirecting one or more sequences to the “yes” exit of block 6.

4.5.3 Enhancing reliability

Non-compliance of a PIE with its RAC at STL may be driven by the low reliability of the demanded safety systems which would negatively affect the success probability for the PIE (Block 9). Increasing the probability of success sequences will eventually allow for fulfilment of the PIE acceptance criteria at STL.

A given sequence may result failed due to the failure of one or more safety systems to start up. A high probability of this type of sequences is an indication of low reliability of safety systems. Low reliability may be driven by independent failures or common cause failures on a system or component, unavailability because of maintenance, or because of human failure.

An efficient way to improve reliability is to identify in the Boolean functions (i.e., the fault tree Boolean product) of failed sequences the cutsets leading to the failure of the safety system and to evaluate the potential reliability improvements by means of an importance analysis. A reliability increase may allow for failed sequence reclassification or even for screening the sequence out. The adequacy of reliability enhancing for a given sequence can only be confirmed when, once reclassified, it complies with safety limit of the new category at ITL or when it can be screened out.

As reliability enhancement works exclusively on probabilities, there is no need for new simulation runs to verify the change. Physical results obtained on the original runs for a given sequence are still valid. At the same time, non-compliance of a reclassified sequence (Block 13) or a non-failed sequence (Block 6) with the next class criteria at ITL cannot be solved by protection reliability enhancement.

Enhancing the reliability of safety systems as a means to get an acceptable design is a corrective measure that can be identified by the EBEPU methodology, but not by traditional DSA methodologies.

4.5.4. Adding a new level of protection.

The two previous alternatives work either on capability or on probability. The third type of corrective measure, i.e., adding a new level of protection, modifies both variables. This is equivalent to the introduction of a new barrier in the defence-in-depth structure. The basic idea is to split the failed sequences so that the introduction of the new safety feature has two benefits. On the one hand the actuation of the new protection drives the originally failed sequence into success and on the other the failed sequence resulting from the failure of the new safety feature will be of lower probability than the originally failed sequence. So two main objectives are found:

a) Increasing the overall success probability

b) Allowing for screening out or reclassification of more failed sequences.

Adding a new level of protection may imply the introduction of a new system but it is also possible to get the same effect by introducing a new protection signal that activates an already existing protection system e.g.: seismic scram.

For the case that a PIE does not fulfil its class criteria at STL (Block 9) addition of a new level of protection will provide a higher success probability and possibly a higher number of excluded sequences.

For the case of a specific failed sequence that originally cannot be reclassified (exit “no” of Block 11), the introduction of the new protection system may allow for getting at least one new sequence complying with the class RAC at STL (Block 10) and to reclassify (Block 11) or screen out (Block 2) the new failed sequence.

When an original sequence is reclassified but no compliance with the new class limits at ITL is achieved (exit “no” of Block 13), the addition of a new protection system may allow for getting in the success side a sequence that does not need to be reclassified because it fulfils the initial class limits at STL (Block 10) or for a sequence that continues to be reclassified but complies with the new class limits at ITL (exit “yes” of Block 13). The lower probability of the new failed branch will hopefully allow for the elimination of this sequence (Block 2).

For the case of a sequence complying with the acceptance criteria at STL, but failing compliance with the next class acceptance criteria at ITL (exit “no” of Block 6), the addition of a new level of protection may allow for compliance of new branches with the next class limits at ITL (exit “yes” of Block 6) and for screening out the new failed branch (Block 2).

In all cases, adding a new level of protection implies that new sequences will appear in the event tree and therefore, new simulation runs need to be run in order to perform the BEPU analysis of the new sequences.

5. Conclusions

E-BEPU Manual (Del 3.8)

E-BEPU is a safety analysis methodology applicable to the analysis of Postulated Initiating Events (PIE) in complex facilities and, in particular, in nuclear power plants. Complex facilities usually encompass some level of risk derived not only from their normal operation but also from possible disturbances that could result in significant damages. Adequate design of production and control systems should limit the damage or unintended effects resulting from normal operation. Limitation of the risks due to disturbances and abnormal operation is the aim of plant protections.

Plant protections are designed on the basis of selected Postulated Initiating Events (PIE) that, along with a set of challenge maximizing assumptions, configure the so-called Design Basis Accidents (DBA). They are used to determine the capabilities of plant protections and their actuation set-points. Traditionally, a main element of the safety analysis supporting the licensing of nuclear power plants has been the verification of the plant protection capability to cope with DBA.

Deterministic methods have been usually applied for such verification. For this reason, licensing safety analyses are often referred to as Deterministic Safety Analysis (DSA). However, different approaches have been used and accepted by regulators. The purely conservative approach was initially required to ensure compliance with licensing safety limits under the design basis assumptions. Later on, other options have been developed that progressively rely on more realistic assumptions while maintaining the necessarily enveloping approach of a safety analysis. Moving towards realism has been encompassed by explicit consideration of uncertainties in the analysis methodologies. In all these approaches, applicable acceptance criteria are linked to the accident class where the PIE is classified.

Best-Estimate Plus Uncertainty (BEPU) methodologies are now widely accepted for the analysis of DBA. In this type of methodologies, simulation of the plant dynamics is based on best-estimate models. Uncertainties are considered in initial and boundary conditions, in properties of the system and in physical models. However, the availability of safety systems, i.e., plant protections, is determined by applying the single failure criterion. As a consequence, DBA usually consist of a single sequence, or a small number of them, triggered by the occurrence of a PIE and involving a predetermined set of protections. For probabilistic BEPU methodologies, the acceptance criteria must be fulfilled with a pre-specified tolerance level, composed by a probability level and a confidence level.

E-BEPU is an extension of the BEPU methodologies with two important improvements. On the one hand, it incorporates uncertainty in the configuration of the safety systems involved in PIE initiated accidents. On the other, it requires compliance with additional acceptance criteria with an increased tolerance level in order to avoid possible cliff-edge effects. Both features contribute to a better implementation of Defence-in-Depth principles.

The E-BEPU approach is supported by the incorporation of analysis techniques typically used in PSA, although the purpose is different. Dynamic event trees are used to identify the possible sequences starting from a PIE and fault tree models encompass the probabilistic quantification of event tree sequences.

It can be concluded that E-BEPU is the result of a sound combination of deterministic and probabilistic techniques, applicable to licensing safety analysis, usually addressed by DSA, in nuclear power plants. Among its unique features, it can be mentioned its ability to check the validity of Design Basis Envelopes and its capability to identify and analyse Design Extension

Conditions. E-BEPU provides also means for verifying Defence-in-Depth aspects in the plant design and preclusion of cliff edge effects.

Defence-in-depth (Del 3.9)

After the Fukushima Daiichi accident the need for revisiting the concept of defence-in-depth became apparent. All international organizations (IAEA, WENRA, EUR) which produce safety standards started to work on this issue immediately following the Fukushima Daiichi accident. Refined structure of the levels of defence-in-depth is included in the IAEA Safety Standards, WENRA Safety of new NPP designs and EUR documents. The table below shows that all standards have the same breakdown of the level 3 of defence-in-depth but they all use different terms to describe the basic concept which is equivalent in all three documents:

Level of defence-in-depth	E.U.R.	IAEA	WENRA Safety of new NPP designs
Level 3a	Design Basis Accidents	Design Basis Accidents	Postulated single initiating events
Level 3b	DEC – Complex sequences	DEC-A without core melt	Postulated multiple failure events
Level 4	DEC – Severe accidents	DEC-B with core melt	Postulated core melt accidents

Table 3.1 Nomenclature for DBA and DEC in different international standards

The IAEA SSR 2/1 Rev 1 in para 4.13A requires that “the levels of defence-in-depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of the other level. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall as far as is practicable be independent of safety systems.” Similar requirement can be found in WENRA Objective 4 “Independence between all levels of defence-in-depth”. IAEA TECDOC-1791 devotes the entire Chapter 6 to the independence of levels of defence-in-depth.

Levels of defence-in-depth have been further elaborated in TECDOC-1791 (Table 5.2). It is just a proposal at the moment but it brings an important question on where to place DEC-A, i.e. design extension condition without core melt, in level 3 or in level 4. One possibility would be to divide level 3 into 3a and 3b, where the objective of 3a would be to control design basis accidents and placing design extension conditions without core melt into the level 3b. Mitigation of consequences in design extension condition with core melt would remain in level 4 of defence-in-depth. The other possibility would be to retain the control of design basis accidents in level 3 and place both design extension conditions (with and without core melt) into level 4 of defence-in-depth.

Therefore the concept of defence-in-depth has been introduced to fulfill the fundamental safety principle that “all practical efforts must be made to prevent and mitigate nuclear or radiological emergencies”. E-BEPU can contribute in this respect by pointing out that analyzing only the worst single failure does not ensure that combination of failures that could give rise to significant harmful effects are of very low probability, which can then lead to a breach in the implementation of defence-in depth. E-BEPU addresses these situations and implement defence-in-depth in a systematic manner by addressing all possible sequences

that can originate from a postulated initiating event and not only the case of the worst single failure.

Additionally, the introduction of new acceptance criteria with a new tolerance level in E-BEPU, in addition to those used in standard BEPU, provides a capability to assess important issues of defence-in depth such as the possibility of cliff-edge effects.

<table>
<tr><th colspan="2">Level of defence Approach 1</th><th>Objective</th><th>Essential design means</th><th colspan="2">Level of defence Approach 2</th></tr>
<tr><td rowspan="2">Level 3</td><td>3a</td><td>Control of design basis accidents</td><td>Engineered safety features (safety systems)</td><td colspan="2">Level 3</td></tr>
<tr><td>3b</td><td>Control of design extension conditions to prevent core melt</td><td>Safety features for design extension conditions without core melt</td><td>4a</td><td rowspan="2">Level 4</td></tr>
<tr><td>Level 4</td><td></td><td>Control of design extension conditions to mitigate the consequences of severe accidents</td><td>Safety features for design extension conditions with core melt. Technical Support Centre</td><td>4b</td></tr>
</table>

Table 5.1 Proposal for two ways of splitting levels 3 and 4 of defence-in-depth (from TECDOC-1791)

These advantages are obtained at the cost of significant increase of computational time but it is presumed that with todays and future computing capabilities it is affordable.

References

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Specific Safety Guide No. SSG-2 Deterministic Safety Analysis for Nuclear Power Plants, IAEA, Vienna (2009).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Report Series No. SRS # 23 on Accident Analysis for Nuclear Power Plants, IAEA, Vienna (2002).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, Safety Fundamentals No. SF-1, IAEA, Vienna (2006).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Specific Safety Requirements No. SSR 2/1 (Rev 1), Safety of Nuclear Power Plants: Design, IAEA, Vienna (2016).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, General Safety Requirements No. GSR Part 4 (Rev 1), Safety Assessment for Facilities and Activities, IAEA, Vienna (2016).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Specific Safety Guide No. SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA, Vienna (2010).

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

[8] US NUCLEAR REGULATORY COMMISSION, Domestic Licensing of Production and Utilization Facilities, Code of Federal Regulations 10, Part 50, US Government Printing Office, Washington, DC (1974).

[9] US NUCLEAR REGULATORY COMMISSION, Regulatory Guide 1.157, Best-Estimate Calculations of Emergency Core Cooling System Performance, Task RS 701-4, Washington, DC (1989).

[10] COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS, CSNI Status Summary on Utilization of Best-Estimate Methodology in Safety Analysis and Licensing, Report NEA/CSNI/R (1996), OECD Nuclear Energy Agency, Paris (1996).

[11] COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS, CSNI Task Group on CSNI Safety Margins Action Plan (SMAP), Final Report, “NEA/CSNI/R(2007)9, May 2007.

[12] Celine Lascar, Joshua L. Parker, both Framatome, ARITA – a new method for safety margin evaluation, ENS Newsletter # 1, January 2019.

[13] ANSI/ANS-51.1-1983, Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants, American Nuclear Society, La Grange Park, Illinois (1983).

[14] KTA-SG-47 (Draft), Zum Konzept: Klassifizierung von Ereignisablaeufen fuer die Auslegung von Kernkraftwerken, Kerntechnischer Ausschuss (KTA), Salzgitter, Germany.

[15] European Utility Requirements for Light Water Reactor Nuclear Power Plants (E.U.R.) Revision E, http://www.europeanutilityrequirements.org, 2016.

[16] WENRA RHWG, Western European Nuclear Regulators Association, Reactor Harmonization Working Group, Safety of new NPP designs, March 2013.

[17] Dusic, M.,Dutton, M., Glaeser, H., Herb, J., Hortal, J., Mendizábal, R., Pelayo, F., Combining Insights from Probabilistic and Deterministic Safety Analyses in Option 4 from the IAEA Specific Safety Guide SSG-2. Nuclear Technology vol. 188 (October 2014) pp. 63-77.

[18] ANSI-N-18.2 Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants, ANSI, January 1975.

[19] R. Mendizábal & F. Pelayo, "BEPU Methodologies and Plant Technical Specifications". Proc. ASME 3rd Joint US-European Fluids Engineering Summer Meeting", Montreal, QC, Canada, 1-5 August 2010, pp. 1573-1579.

[20] S.S. Wilks, "Determination of sample sizes for setting tolerance limits", The Annals of Mathematical Statistics, 12, No 1, 1941, pp. 91-96.

[21] S. S. Wilks, "Order Statistics", *Bull. Amer. Math. Soc*., Volume 54, Number 1, Part 1, 1948 pp. 6-50.

[22] R. Mendizábal , "Verifying the fulfilment of acceptance criteria: Initiating Events and Sequences", *IAEA Technical Meeting on Best Estimate Plus Uncertainty (BEPU) in Safety Analyses*, Pisa (Italy), 10-14 June 2013.

[23] R. Mendizábal, "Some insights on the fulfilment of acceptance criteria by finite mixtures", *ANS Best Estimate Plus Uncertainty International Conference (BEPU 2018)*, BEPU2018-125, Real Collegio, Lucca, Italy, 13-19 May 2018.

[24] Amended Nuclear Safety Directive on 8 July 2014 (Directive 2014/87/Euratom)

[25] Vienna Declaration on Nuclear Safety, CNS/DC/2015/2/Rev.1, IAEA 2015.

[26] S. Martorell et al., An approach to address probabilistic assumptions on the availability of safety systems for deterministic safety analysis, Reliability Engineering and System Safety 160, pp.136-150, 2017.

[27] S. Martorell et al., An extended BEPU approach integration probabilistic assumptions on the availability of safety systems in deterministic safety analysis, Reliability Engineering and System Safety 167, pp.474-483, 2017.

[28] WENRA RHWG, Western European Nuclear Regulators Association, Reactor Harmonization Working Group, Safety Reference Levels for Existing Reactors, September 2014.