NARSIS

New Approach to Reactor Safety ImprovementS

WP3: Integration and Safety Analysis

Del3.10 – Use of Extended Best Estimate Plus Uncertainty (E-BEPU) methodology for Evaluation of Design Extension Conditions (DEC)

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:	Del3.10 – Use of E-BEPU for evaluation of Design Extension Conditions		
Month due:	M36	**Month delivered:**	M35
Leading Partner:	NUCCON GmbH		
Version:	Final V1		

Primary Author: Milorad DUSIC and Javier HORTAL (NUCCON)

Other contributors:

Deliverable Review:

- **Reviewer #1:** Ivica Basis, Ivan Vrbanic – APOSS **Date:** 03/2020
- **Reviewer #2:** Piotr Mazgaj, Piotr Darnowski – WUT **Date:** 03/2020

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

AOO	Anticipate Operational Occurrences
BE	Best Estimate
BEPU	Best Estimate Plus Uncertainty
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
DSA	Deterministic Safety Analysis
E-BEPU	Extended Best Estimate Plus Uncertainty Analysis
ECCS	Emergency Core Cooling System
E.U.R.	European Utility Requirements
IAEA	International Atomic Energy Agency
ITL	Increased Tolerance Level
LP	Low Pressure
NO	Normal Operation
NPP	Nuclear Power Plant
NS	Nuclear Safety
P/C	Probability vs. Consequences
PIE	Postulated Initiating Event
PS	Plant States
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
RHR	Residual Heat Removal
SAR	Safety Analysis Report
SSG	Specific Safety Guide
SSR	Specific Safety Requirements
STL	Standard Tolerance Level
TMI	Three Mile Island
WENRA	West European Nuclear Regulators' Association

1 Executive Summary

Traditionally, licensing of nuclear power plants (NPP) has put a special focus on safety systems, their design basis and their performance. Consequently, strict licensing rules apply to the selection of Design Basis Transients and Accidents (DBT and DBA) for safety systems and to performance of safety systems under design basis conditions. Despite the special attention devoted to safety systems, it was very soon realized that they were not the only safety concerns in NPP. The Three Mile Island accident confirmed that more attention should be payed to situations escaping the design basis of safety systems. From the point of view of design requirements, the licensing scope is also being enlarged. Progressively, more attention is being payed to the design of non-safety systems and to other elements and features such as accident management issues, although the level of enforcement is not always the same as for safety systems. The concept of “Design Extension” is being increasingly considered in licensing requirements, replacing the more traditional term “Beyond Design Basis”, which suggests something not to be taken into account.

The Extended Best Estimate plus Uncertainty (E-BEPU) methodology has been developed as an improved approach to the analysis of design basis accidents. So far, the most advanced methodologies for verification of the design of safety systems are those based on the use of best-estimate simulation models and assumptions complemented with an uncertainty analysis. They are usually referred to as BEPU methodologies. The main feature of E-BEPU is to extend the scope of the uncertainty analysis to include the availability of safety systems as an additional uncertain item. This implies to incorporate risk insights in a traditionally deterministic analysis environment.

This report gives details on the use of E-BEPU in addressing the Design Extension Conditions (DEC). The main element of E-BEPU is the use of the acceptance criteria with the Increased Tolerance Level (ITL) for the next higher class. However for Postulated Initiating Events belonging to the highest class of design basis accidents (DBC-4), there is no higher class in the safety design basis space. Nevertheless, considering the graded approach to safety analysis above described, DEC conditions can be seen as additional classes for safety analysis and, in particular, DEC-1 can be considered as the “next higher class” of the highest class of DBA. While in DBA moving from one class to other only implies a change in the acceptance criteria, in applying the E-BEPU methodology to the highest class in the design basis space, means moving from DBA to DEC where also the analysis requirements might need to be changed. Moreover, the acceptance criteria in terms of barrier degradation could be actually the same for DBA and DEC-1, changing only the analysis requirements.

In the E-BEPU process, when we verify if the sequence fulfills the acceptance criteria with the ITL of 99/95, means that we are analyzing a successful sequence, i.e., a sequence that, with the only intervention of safety systems, meets the acceptance criteria in at least 95% of cases. In the case that the percentage of successful runs is lower than 99% we would have to classify the design as unacceptable. However, the “next class” is no longer a DBA class and the analysis requirements are different. Thus, for the purpose of checking fulfillment of acceptance criteria with ITL it is allowed to take into account other safety features additional to automatic safety systems, e.g., operator actions guided by emergency procedures. If those actions are effective to avoid exceedance of the acceptance criteria in a significant number of cases, the analysis of that sequence would be acceptable. The analysis of such a sequence gives acceptable results if the exclusive response of safety systems avoids exceeding the acceptance criteria in at least 95% of cases and if the combined response of safety systems and additional safety features avoids such exceedance in at least 99% of cases (always requiring a 95% confidence level).

Something similar occurs in the case of sequence reclassification into the next higher class due to its low probability of occurrence. Here, it can happen that the analyzed sequence is not successful, i.e., it does not fulfill the initial class acceptance criteria with STL or, in other words, by relying only on safety systems, the acceptance criteria are exceeded in more than 5% of

cases. However, its probability is low enough as to reclassify it to the next class, i.e., to DEC-1. Then, the analysis of this sequence will give acceptable results if safety systems along with other safety provisions for DEC-1 are able to fulfill the acceptance criteria in at least 99% of cases.

In any of the above two cases, when this conclusion that “the design is not acceptable” comes from failure to fulfill DEC criteria, the design improvement should not necessarily apply to safety systems. The remedial actions, namely, improvement of performance, improvement of reliability and addition of a new level of protection, would apply to safety features for DEC.

The practical application of E-BEPU will be described in Deliverable 4.5.

2 Introduction

Since the beginning of the development of commercial nuclear energy, safety of nuclear power plants (NPP) has been a concern. In order to make plants acceptably safe, confinement barriers able to prevent the release of radioactive material have been introduced as an essential element of the design. In addition, safety systems are also incorporated with the purpose of preventing or mitigating unacceptable degradation of confinement barriers upon occurrence of abnormal events.

Safety systems are designed to be able to cope with a wide spectrum of possible plant disturbances. Upon occurrence of an abnormal event, triggering a dangerous transient or an accidental situation, one or more safety systems are called for intervention in order to avoid further degradation that could result in a radioactive release.

Every component, system or structure of a facility is designed to comply with a set of specifications that constitute its design basis. The design of safety systems is based on the selection of a reduced set of enveloping events, transients and accidents that result in the most demanding conditions that safety systems must deal with. They constitute the design basis of the safety systems.

Traditionally, licensing of NPP has put a special focus on safety systems, their design basis and their performance. Consequently, strict licensing rules apply to selection of Design Basis Transients and Accidents (DBT and DBA) for safety systems and to performance of safety systems under design basis conditions. In a licensing context, the focus on safety systems is so strong that the terms “design basis” or “plant design basis” are very often used instead of the more accurate terms “design basis of safety systems” or “design basis for plant safety”. In some cases, this simplified terminology may cause some level of confusion.

Despite the special attention devoted to safety systems, it was very soon realized that they were not the only safety concerns in NPP. The Three Mile Island (TMI) accident confirmed that more attention should be payed to situations escaping the design basis of safety systems. The development, implementation and consolidation of Probabilistic Safety Assessments (PSA) is a clear example of the extension of the licensing scope.

From the point of view of design requirements, the licensing scope is also being enlarged. Progressively, more attention is being payed to the design of non-safety systems and to other elements and features such as accident management issues, although the level of enforcement is not always the same as for safety systems. The concept of “Design Extension Conditions (DEC)” is being increasingly considered in licensing requirements, replacing the more traditional term “Beyond Design Basis” which suggests something not to be taken into account. This concept has been extensively considered and elaborated in the IAEA Safety Requirements SSR-2/1 (Rev. 1) [1].

So far, the most advanced methodologies for verification of the design of safety systems are those based on the use of best-estimate simulation models and assumptions complemented with the uncertainty analysis. They are usually referred to as Best Estimate plus Uncertainty (BEPU) methodologies. The Extended BEPU (E-BEPU) methodology has been developed as an improved approach to the analysis of DBA [2]. The main feature of E-BEPU is to extend the scope of the uncertainty analysis to include the availability of safety systems as an additional uncertain item. This implies to incorporate risk insights in a traditionally deterministic analysis environment.

One of the potentialities of the E-BEPU methodology is its ability to address Design Extension issues as discussed in this paper. It will be shown that DEC-A, the Design Extension Condition without core melt and DEC-B, the Design Extension Condition with core melt can be treated as the “next higher class” for the purpose of determination of acceptance criteria or for sequence reclassification.

In order to lay ground for the discussion on the use of E-BEPU in the Design Extension Conditions a very brief summary of the main elements of E-BEPU will be outlined, mostly taken from NARSIS Deliverable 3.8 – Development and Description of E-BEPU Method – Part A "theoretical basis", see reference [3].

The practical application of E-BEPU will be described in Deliverable 4.5.

3 Design extension conditions

3.1 Design extension conditions in the international safety requirements

Plant states (PS) that are considered in the design of NPPs are defined identically in all international standards but with different titles/names and it is therefore prudent to show the equivalence among different definitions.

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

- Normal operation
- Anticipated operational occurrences

For design basis accidents and design extension conditions the concepts in all three documents are the same but different names are used for the corresponding conditions as summarized in the below table for DEC.

SSR 2/1 Req. 20 deals with the Design Extension Conditions (DEC). It specifies that a set of DEC shall be derived on the basis of engineering judgement, DSA and PSA for the purpose of further improving the safety of the NPP by enhancing plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than DBA or that involve additional failures. These DEC shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences. Even though the basic concepts in the IAEA SSR 2/1, E.U.R. and WENRA Safety of new design are the same, the titles given to individual parts of DEC are different in those three requirements documents. The Table 1 depicts the names used by E.U.R., IAEA and WENRA to describe different stages in DEC.

Table 1: DEC definitions in different International Safety Standards

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

SSR 2/1 Req. 20 para 5.27 requires that the safety analysis for DEC be performed but allows (in the footnote) that Best Estimate (BE) approach be used. BE approach can be used also for the analysis of the effectiveness of provisions to ensure the functionality of the containment.

The same para 5.27 further defines that the main technical objective of considering DEC is to provide assurance that the design of the plant is such as to prevent accident conditions that are not considered in design basis accidents or to mitigate their consequence. For this an additional safety features are necessary or the extension of capabilities of existing safety systems.

SSR 2/1 Req. 20 para 5.28 defines that the design specifications for safety features be derived from DEC.

SSR 2/1 Req. 20 para 5.29 makes requirements for safety features to be used in DEC. They are required to:

- Be independent, to the extent practicable, of those used in more frequent accidents.
- Be capable of performing in the environmental conditions pertaining to DEC.
- Shall have reliability commensurate with the functions that they are required to fulfil.

SSR 2/1 Req. 20 para 5.30 requires the containment and its safety features to be able to withstand extreme scenarios including core melt and that these scenarios shall be selected using engineering judgement and inputs from PSA.

SSR 2/1 Req. 20 para 5.31 requires that the design be such that the possibility of conditions arising that could lead to an early radioactive release or large radioactive release be practically eliminated. For accident sequences leading to core melt, that have not been practically eliminated, design provisions shall be taken so that:

- only limited protection measures in area and time are needed for the public
- sufficient time is available to implement these measures.

SSR 2/1 Req. 20 para 5.31A requires that design shall be such that in case of DEC, protective actions limited in terms of length of time and areas of application shall be sufficient. E.U.R. also state that for severe accidents, targets are set to avoid the need of significant off-site protective actions consistently with WENRA's safety objective O3. Criteria for limited impact of severe accidents would lead to limited social consequences.

3.2 Design extensions and design improvements

Not any type of disturbance in a NPP should be considered for determining the design basis of safety systems. Usually, events included under the design basis scope are those triggered by credible or postulated initiating events occurring from expected operating conditions and involving no more than a single failure, additional to the initiating event. Other events, for example those involving multiple independent failures, are left out of the design basis scope.

When developing a safety design the last step must be always checking whether the designed safety systems, with their capabilities and initiation criteria, are able to cope with any event covered by the safety design basis. Otherwise, the safety design must be improved. Possible improvements range from changes in the capabilities or initiation criteria up to introduction of new safety systems.

In the literature about safety of NPP, the term "Design Extension" has not been always used in an unambiguous way. Examples can be found where it refers to design improvements consisting of introducing new safety systems when a deficient coverage of the safety design basis has been identified. It could be acceptable in plain language to call "design extension" the process of enlarging the safety design until it is able to achieve the desired goals. However, this term is being increasingly used to designate specific classes of plant conditions not covered by the safety design basis but involving significant challenges to plant safety. The evident safety significance of Design Extension Conditions (DEC) is resulting in a growing attention to them in regulatory activities. This concept of DEC was introduced in the IAEA standards in 2012 when the Safety Requirements publication "Safety of Nuclear Power Plants: Design" was issued as IAEA Safety Standard Series, Safety Requirements SSR-2/1 and further revised as Safety Requirements SSR-2/1 (Rev.1) in 2016 [1].

DEC are beyond the scope of the safety design basis. But this only means that safety systems are not enough to control and mitigate disturbances leading to those plant conditions. It does not mean that they can be ignored. The term "DEC" suggests that some means, additional to the safety systems, should be provided to cope with this type of disturbances.

When trying to assess the safety of an NPP we can find that some scenarios matching the safety design basis assumptions, i.e., that should be adequately managed by safety systems, result in unacceptable consequences even though safety systems perform as expected. This is a design deficiency that must be corrected by a design improvement. In addition, we can find scenarios that, while exceeding the safety design basis assumptions (therefore, reliance only on safety systems is not enough to avoid undesired consequences), their occurrences are likely enough as to consider them safety significant. This is the case of DEC scenarios

where other safety features, additional to safety systems, can be taken into consideration for safety demonstration.

4 Design basis and design extension: A graded approach to safety analysis

Nowadays it is widely accepted that safety of NPPs cannot rely only on (mostly automated) safety systems. The safety design cannot be indefinitely enlarged to cover any type of scenario with potentially unacceptable consequences. Scenarios escaping the safety design basis envelope need to be analyzed but requirements, assumptions and acceptance criteria can be different from those of the design basis safety analysis.

Design Extension Conditions are plant categories, additional to those traditionally used for Design Basis Transients and Accidents, where acceptance criteria as well as performance and requirements of systems performing safety functions may differ from those applicable to DBA. With the introduction of the concept of DEC, the traditional scope of safety analysis gets enlarged to cover all types of plant conditions with the only exception of extremely unlikely or impossible scenarios.

The introduction of DEC conditions in SSR-2/1 provides a good example of a comprehensive approach to design of NPP where design provisions are checked not only against DBA but also against conditions beyond the design basis of safety systems where other systems are considered as additional means to cope with accidents. This results in a graded approach to nuclear safety where different levels of rules and requirements are applied depending on the likelihood and/or severity of the plant conditions resulting from the occurrence of abnormal events. Plant categories defined in SSR-2/1 cover all types of plant conditions except those that can be considered "practically eliminated"[1].

The implementation of the graded approach consists of requiring more restrictive conditions in terms of acceptance criteria and analysis requirements for events with higher likelihood. For example, taking as a reference the plant categories defined in SSR-2/1 the different levels of requirements could be as follows:

- In Normal Operation (NO) no barrier degradation is allowed. Safety systems are not involved in normal operation with the exception of some systems that, with the same equipment but different operating modes, are able to perform normal functions in normal operation and safety functions in abnormal conditions. An example is the Residual Heat Removal (RHR) System in PWR plants that may also work as Low Pressure (LP) Emergency Core Cooling System (ECCS).
- In Anticipated Operational Occurrences (AOO), the requirements regarding barrier degradation are the same as for NO. However, some safety systems, particularly the reactor trip system, are required to perform their safety functions. Safety systems are automatically initiated (with very few exceptions matching strict conditions) and must be designed to ensure that a single failure does not prevent them from achieving their safety function.
- For design basis accidents (DBA), not all the safety barriers maintain their integrity. Actually, some of these accidents are initiated by a failure of the reactor coolant pressure boundary. As in the case of AOO, only safety systems are credited to lead the plant conditions to an acceptably safe state. A limited degradation of the fuel barrier is allowed but degradation of the containment barrier or consequential degradation of the reactor coolant pressure boundary are not allowed.
- DEC-1 is a plant category where safety systems may not be able to prevent, by themselves, the transition to severe accident. However, with the help of other systems, possibly initiated by operators, this objective can be achieved. The acceptance criteria

[1]In the IAEA safety standards and, in particular, in SSR-2/1 it is said that "*The possibility of certain conditions arising may be considered to have been 'practically eliminated' if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise.*"

in terms of barrier degradation could be the same as for design basis accidents but the analysis requirements are different. Non-safety systems are not required to withstand a single failure, operator actions are taken into account and the use of best-estimate assumptions and models can be more flexible than in the case of design basis accidents. The level of regulatory enforcement can also be lower for DEC than for DBA.

- For DEC-2, the analysis requirements are similar as for DEC-1 but the only barrier required to maintain its integrity is the containment. The main objective is to prevent a prompt or large release of radioactive material.

This graded approach provides a balanced protection environment that adequately combines risk limitation and defense-in-depth (DiD). The Use of E-BEPU for the Evaluation of DiD is fully described in Ref. [4].

5 The E-BEPU approach to analysis of postulated events

Design and verification of safety systems has been always a focus of attention of safety regulations for NPPs. Traditionally, deterministic methodologies have been applied to the analysis of Postulated Initiating Events (PIE) that were used as design basis events for safety systems. This type of safety analysis has been usually referred to as Deterministic Safety Analysis (DSA) and has been always an important part of Safety Analysis Reports (SAR).

DSA is essentially an analysis of envelopes. PIEs that include both AOOs and DBAs, along with some analysis assumptions trying to magnify the effects of the PIE, represent the most demanding conditions that safety systems must be able to manage and define both the design specifications of safety systems and the analysis cases of DSA. Determination of these analysis cases involves a significant amount of qualitative and generic arguments. Successful results of the analysis allow to verify that safety systems meet the design specifications but they typically provide poor indications on whether the safety envelope has been correctly defined and, therefore, whether the design specifications are adequate.

At a first glance, DSA methodologies based on highly conservative assumptions and methods seem to provide more confidence on the adequacy of the envelope because they involve large safety margins. This is not always a correct assumption because in some cases the excessive conservatism may produce a masking effect of safety significant phenomena. Using more realistic models and assumptions tends to provide better adjusted envelopes but, at the same time, the possibility that some special occurrences could escape the design envelope is more likely. For this reason, using best-estimate models and assumptions for DSA is only allowed if they are complemented by an uncertainty analysis.

Most of BEPU methodologies use statistical methods to perform the uncertainty analysis assuming that uncertain parameters can be characterized by probability distributions. This type of approach has the beneficial side effect that the uncertainty analysis is, at the same time, a sensitivity analysis. A Design Basis Accident, i.e., a PIE with its associated magnifying assumptions, is assumed to represent a point inside the safety envelope but very close to it. When performing the sensitivity/uncertainty analysis, a number of cases are run by randomly sampling uncertain parameters. Each run represents a point in the design basis space near the nominal point of the DBA. Runs fulfilling the acceptance criteria of the DBA represent points inside the envelope. Runs not fulfilling those criteria represent points outside the design envelope. Therefore, the sensitivity/uncertainty analysis implies a more complete verification of the envelope, not limited to a single case for each DBA. The more extensive the sensitivity/uncertainty analysis, the better verification of the envelope there is in the vicinity of the DBA.

The uncertainties that are typically considered in BEPU methodologies are related with simulation model parameters or initial and boundary conditions for the analysis cases. One of the main features of E-BEPU [2] is that it extends the scope of the uncertainty analysis to include also the configuration of safety systems. This type of uncertainty is addressed by systematic analysis instead of random sampling.

Possible failures of safety systems need to be and have been always considered because in normal operation they are in stand-by, waiting for activation upon occurrence of a plant disturbance. Although they are systematically tested to prevent failures, initiation of the safety system is a sudden change that could induce a failure or could reveal a hidden failure that occurred after the last surveillance test. This is taken into account in the design phase by making safety systems resistant to a single failure and in the traditional DSA by assuming that the configuration of safety systems is the one resulting from the occurrence of the worst single failure in the course of an accident.

By enlarging the scope of the uncertainty analysis, E-BEPU pursues a double goal. On the one hand, E-BEPU helps to improve the verification of the safety envelope by applying the analysis in a larger environment around the nominal DBA. On the other, it helps to identify

some design weaknesses that are not evident when using traditional methods. In the E-BEPU approach, all the possible safety system configurations resulting from different combinations of failures (including the no-failure case) are systematically explored. Among them, only those being very unlikely are discarded with the exception of single failure configurations that are always retained. E-BEPU is the result of incorporating risk insights and PSA methods into DSA. The main features of E-BEPU and its application steps are summarized in next section.

6 A brief description of the E-BEPU methodology

The E-BEPU methodology is fully described in NARSIS Deliverable 3.8 Ref. [3]. In this section, brief elements of E-BEPU which are important for understanding the reminder of this paper are presented in order to lay ground for the full explanation of the use of E-BEPU for DEC.

The most important characteristics of E-BEPU as compared with existing BEPU methodologies are the systematic consideration of all the possible safety system configurations, the reclassification of sequences and the use of second-level acceptance criteria additional to those applicable to the analyzed DBA.

In traditional DSA, each DBT/DBA is initiated by a PIE and continues with the activation of the necessary safety systems to control the situation. The DBT/DBA is typically represented (with few exceptions) by a single sequence of events that includes the worst single failure in safety systems. The PIE that initiates the accident determines the class of the accident and, therefore, the acceptance criteria for the analysis results. The E-BEPU approach consists of starting from the same PIE but considering all the possible accident sequences that result from different configurations of safety systems. After a screening process, classical BEPU analysis is applied to each individual sequence.

The class of the PIE is the same as in traditional DSA but this class is not necessarily the same for all the sequences resulting from the PIE. Some sequences corresponding to low probability configurations can be reclassified to a higher class with the consequence of changing the applicable acceptance criteria.

For non-reclassified sequences, the applicable acceptance criteria are, initially, those corresponding to the PIE class. As in classical BEPU, a tolerance level is defined to check compliance with those criteria. However, E-BEPU goes further by requiring not only compliance with the standard acceptance criteria at the Standard Tolerance Level (STL) but also compliance with the acceptance criteria corresponding to the next higher class, using an Increased Tolerance Level (ITL). This way, some cliff-edge effects that remain hidden in classical DSA can be identified in E-BEPU. The typical value of STL is the one used in classical BEPU i.e., 95/95 (coverage/confidence). No value for ITL can be considered typical but 99/95 has been proposed for application exercises.

Figure 1, taken from [2], represents the application process of E-BEPU to a particular PIE. The first step (Block 1) is to determine the class to which the PIE belongs and therefore the acceptance criteria that should be initially used.

In Block 2, the sequences resulting from the PIE are identified and their probabilities are quantified based on the safety system configuration that each sequence represents. Sequences with very low probability, below a defined cutoff value, are screened out. These sequences are discarded for the analysis but it must be checked that the cumulative probability of all the discarded sequences is still below the cutoff value.

A classical BEPU analysis is then performed for each retained sequence (Block 3). If all the sequences are found to fulfill the initial acceptance criteria with STL, the analysis continues through the left branch of the diagram.

In Block 5, the acceptance criteria that apply to the next higher class of the PIE are identified and the analyzed sequences are checked to fulfill those criteria with ITL. Failure to do that (exit “no” of block 6) is an indication of a possible cliff-edge effect and, therefore, an indication of a design deficiency that would not have been identified by classical DSA.

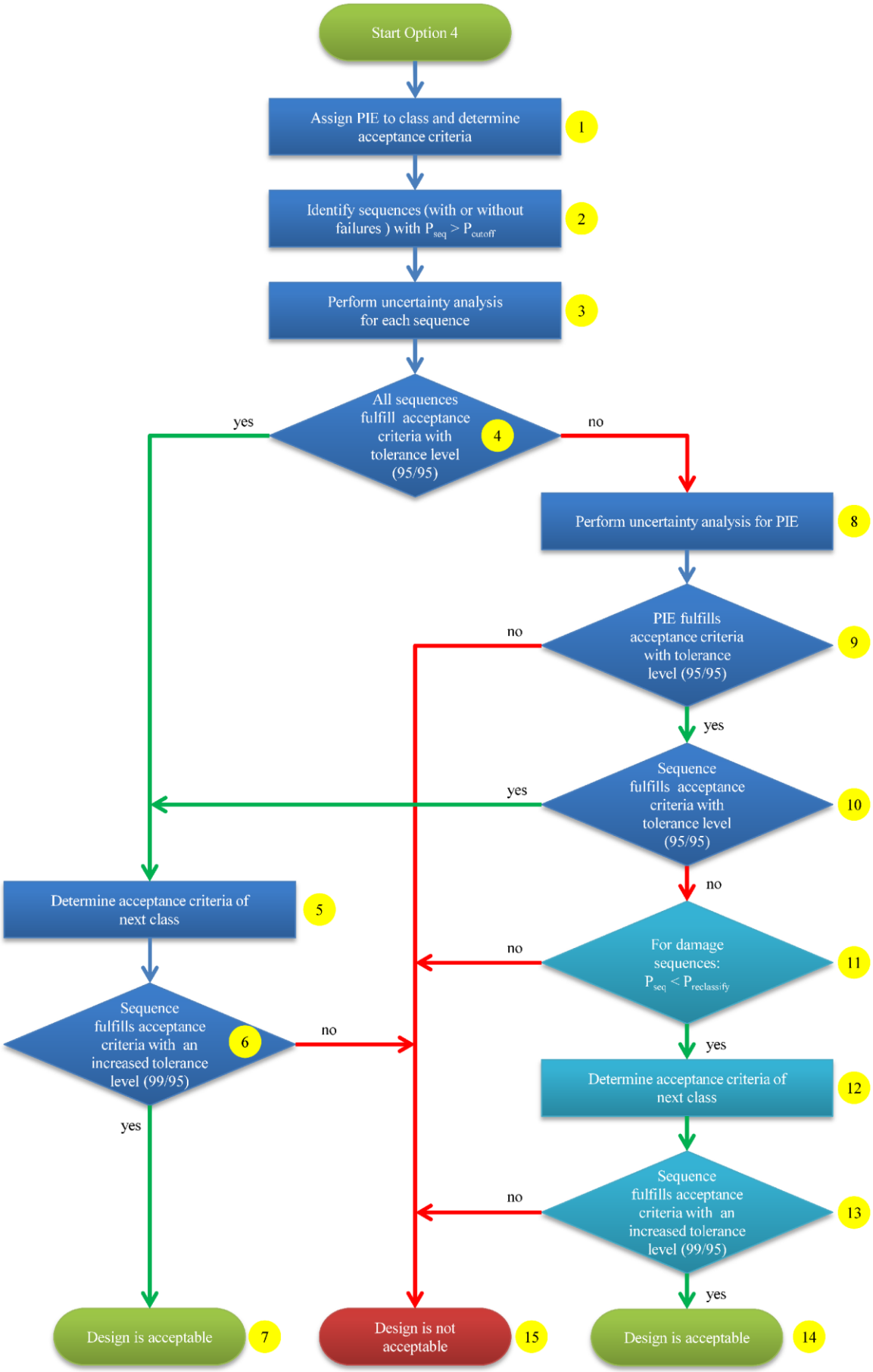

Figure 1: Flow diagram of the E-BEPU methodology

If there are failed sequences, i.e., sequences not fulfilling the acceptance criteria of the PIE class with STL the analysis flow is directed towards the right branch of the diagram. First, it is checked whether considering all the sequences together it can be concluded that at the level of the whole PIE the acceptance criteria are met with STL. If not (exit “no” of Block 9), it can be concluded that the design is deficient.

Otherwise, successful sequences are redirected to Block 5 and processed as explained above. For failed sequences, it is checked if they can be reclassified, i.e., if their probability is lower than a defined threshold value. If not, it is concluded that there is some design deficiency. If reclassified, it is considered that fulfilling the next class criteria with ITL is a sufficient condition to consider them acceptable but failing this condition is also an indication of a design deficiency.

7 Transition from DBA to DEC-1 with E-BEPU

The above description of E-BEPU applies to the general case of a PIE belonging to an intermediate class of DBAs. Design deficiencies identified in the analysis of this type of PIE need to be solved by improving the safety design. Depending on the specific type of deficiency, one or more of the following design improvement methods can be applied:

- Improving the safety system performance by increasing system capabilities, e.g., by using more powerful pumps able to deliver more flow.
- Improving the safety system reliability in such a way that the probability of failed sequences gets lower up to the point that they can be either reclassified or screened out.
- Adding a new level of protection, i.e., adding new safety systems with capability to avoid failure in previously failed sequences. By using this method, failed sequences are split in at least two sequences, one where the new system performs as expected and leading to success and one or more corresponding to failures of the new system and possibly going to failure but with probabilities much lower than the original failed sequence.

For the first case of improvement of the safety system 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.

For enhancing the reliability of safety systems, 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.

It is worth to point out that enhancing the reliability of safety systems as a means to get an acceptable design is a corrective measure that can be identified by the E-BEPU methodology, but not by traditional DSA methodologies.

For the third case of addition of a new level of protection, it 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.

In this third case, we are adding a new level of protection. 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.

More on these three options have been presented in the NARSIS Deliverables 3.8 and 3.9 pages 56-58 [3, 4].

The case of a PIE belonging to the highest class of DBA needs some more discussion because, in this case, there is no “next higher class” in the safety design basis space. Nevertheless, considering the graded approach to safety analysis above described, DEC conditions can be seen as additional classes for safety analysis and, in particular, DEC-1 can be considered as the “next higher class” of the highest class of DBA.

However, this extension of the safety analysis scope has important implications. Let us consider a PIE belonging to the highest class of DBA which is being analyzed with E-BEPU. Successful sequences will reach at some moment blocks 5 and 6 of the flow diagram (Figure 1). Failed sequences may reach also blocks 12 and 13 if they are reclassified. In these cases, what should be understood by “acceptance criteria of the next class”? While in DBA moving from one class to other only implies a change in the acceptance criteria, moving from DBA to DEC means to change also the analysis requirements. Moreover, as indicated in section 3 above, the acceptance criteria in terms of barrier degradation could be actually the same for DBA and DEC-1, changing only the analysis requirements.

It must be recalled that the analysis of DBA assumes that all the safety functions needed to mitigate and terminate the accident are performed only by safety systems initiated by automatic signals (with few exceptions). In the analysis of DEC, however, additional safety features can be considered, including operator actions.

According to this, blocks 5 and 12 of the block diagram should be interpreted as “Determine the acceptance criteria and analysis requirements of the next class”. Then, application of blocks 6 and 13 should be consistent with this interpretation. In the case of similar acceptance criteria and different analysis requirements they are applied as follows.

Reaching block 6 means that we are analyzing a successful sequence, i.e., a sequence that, with the only intervention of safety systems, meets the acceptance criteria in at least 95% of cases. Let us assume that, nevertheless, the percentage of successful runs is lower than 99. Since the PIE being analyzed belongs to the highest class of DBA, the “next class acceptance criteria” are those of DEC-1, i.e., the same of the initial class. With the analysis requirements of DBA, this sequence would not fulfill the next class acceptance criteria with ITL and we should leave Block 6 through the “no” exit. However, the “next class” is no longer a DBA class and the analysis requirements are different. Thus, for the purpose of checking fulfillment of acceptance criteria with ITL it is allowed to take into account other safety features additional to automatic safety systems, e.g., operator actions guided by emergency procedures. If those actions are effective to avoid exceedance of the acceptance criteria in a significant number of cases, the analysis of that sequence would be acceptable and the exit from Block 6 of the diagram would be through the “yes” branch. In summary, the analysis of such a sequence gives acceptable results if the exclusive response of safety systems avoids exceeding the acceptance criteria in at least 95% of cases and if the combined response of safety systems and additional safety features avoids such exceedance in at least 99% of cases (always requiring a 95% confidence level).

Something similar occurs in Block 13. In this case, the analyzed sequence is not successful, i.e., it does not fulfill the initial class acceptance criteria with STL or, in other words, by relying only on safety systems, the acceptance criteria are exceeded in more than 5% of cases. However, its probability is low enough as to reclassify it to the next class, i.e., to DEC-1. Then, the analysis of this sequence will give acceptable results if safety systems along with other safety provisions for DEC-1 are able to fulfill the acceptance criteria in at least 99% of cases.

In any of the two cases, i.e., leaving Block 6 or Block 13 through the “no” exit, Block 15 is reached where it is concluded that “Design is not acceptable”. However, when this conclusion comes from failure to fulfill DEC criteria, the design improvement should not necessarily apply to safety systems. The three types of remedial actions listed above, namely, improvement of performance, improvement of reliability and addition of a new level of protection, would apply, preferably, to safety features for DEC.

8 Application of E-BEPU in DEC

The E-BEPU methodology does not only allow for identifying DEC scenarios derived from the analysis of DBA, it also provides additional insights. In the context of the graded approach to safety analysis DBA and DEC are just different types of accident classes, each one with its own characteristics and E-BEPU provides enough flexibility as to apply it for both types of scenarios.

As discussed in the previous sections, safety systems are designed on the basis of limiting AOO and DBA that allow defining their design specifications. For DEC scenarios, safety systems are still available but they are not expected to be sufficient. Other safety features need to be added and, therefore, they need to be designed. Design techniques may be very different for safety systems and safety features for DEC. Selection of design basis scenarios may be based on different criteria for DBA and DEC. However, it is clear that every safety feature for DEC must be designed on the basis of one or more accident scenarios belonging to the DEC class where that feature is assumed to work.

Another difference between design of safety features for DEC and design of safety systems is that the latter need to comply with much stronger regulatory requirements. Although some requirements are being imposed for DEC, they do not have the same level of enforcement and uniformity among different countries. As a result, design and verification of safety systems is much more standard while design and verification of safety features for DEC is more flexible.

Anyway, if the design scenario (defined by a PIE and a set of analysis assumptions) for a given safety feature is well identified, E-BEPU can be applied to verify the actual effectiveness of that feature to cope with that scenario and some of their variants. Moreover, even if the design basis scenario is not identified but the safety feature is known to be required in a particular type of scenario (also defined by an initiating event and some additional assumptions), E-BEPU can be applied for the analysis of that particular scenario.

With regard to acceptance criteria in DEC categories, they were briefly discussed in section 3 above. Basically, the objective of protective features in DEC-1 is to avoid transition to severe accident, i.e., to maintain the global integrity of the fuel barrier (limited local damage can be allowed) and also the integrity of containment. This results in acceptance criteria which are essentially similar to those of the highest class of DBA. In DEC-2 the only barrier required to maintain its integrity is the containment and the final objective is to avoid early or large releases to the outside.

When analyzing a DEC-1 scenario the flow diagram of Figure 1 is fully applicable, changing requirements and parameters as needed. For example, the level of coverage provided by safety features can be lower than in the case of safety systems. In the DBA case, a sequence is typically considered successful if the acceptance criteria are fulfilled with a 95% probability and a 95% confidence. For DEC scenarios, both the probability and the confidence level could be lower and, therefore, the definition of STL and ITL could be different. Other parameters such as cutoff of reclassification probabilities can be different as well and the requirement to retain any single failure sequence in the screening process of Block 2 could be relaxed. Acceptance criteria for the initial class (DEC-1) and for the next class (DEC-2) exist and can be applied. Reliability of safety features is expected to be lower than that of safety systems and, in many cases, these features could not be single failure resistant. However, none of these changes modify the analysis procedure represented in Figure 1.

In the case of DEC-2 scenarios the difficulties that were outlined in section 6 for the case of PIE in the last class of DBA arise again with the added circumstance that DEC-2 is really the very last class of the safety analysis scope. For DEC-2 the concept of “next class acceptance criteria” does not even exist. Therefore, the application of blocks 5-6 and 11-13 needs to be discussed. It must be recalled that plant categories defined in SSR-2/1 and similar standards cover all types of plant scenarios except those that can be considered “practically eliminated” (see footnote 1). In the context of an E-BEPU analysis, it must be ensured that the very last

acceptance criteria, i.e., those of DEC-2, are exceeded only in sequences matching the definition of “practically eliminated” which, in this case, reduces to extremely unlikely sequences; i.e. probability of extremely unlikely sequence < probability of practically eliminated sequences.

Blocks 5 and 6 are applied to successful sequences, i.e., sequences where acceptance criteria are fulfilled with STL. If the STL is P/C (P = coverage probability; C = confidence level), a successful sequence may result in exceedance of the acceptance criteria with probability 1-P. Thus, the STL applied to DEC-2 sequences must be such that 1-P multiplied by the sequence frequency allows qualifying the limit exceedance as extremely unlikely.

Blocks 11-13 correspond to reclassified sequences. In DEC-2, reclassifying a sequence means, in practice, that the sequence is not further analyzed. In consequence, the reclassification probability should be such that reclassified sequences can be considered extremely unlikely.

9 Conclusions

The main element of E-BEPU is the use of the acceptance criteria with the Increased Tolerance Level for the next higher class. However for Postulated Initiating Events belonging to the highest class of design basis accidents (DBC4), there is no higher class in the safety design basis space. Nevertheless, considering the graded approach to safety analysis above described, DEC conditions can be seen as additional classes for safety analysis and, in particular, DEC-1 can be considered as the “next higher class” of the highest class of DBA. While in DBA moving from one class to other only implies a change in the acceptance criteria, in applying the E-BEPU methodology to the highest class in the design basis space, means moving from DBA to DEC where also the analysis requirements might need to be changed. Moreover, the acceptance criteria in terms of barrier degradation could be actually the same for DBA and DEC-1, changing only the analysis requirements.

In the E-BEPU process, when we verify if the sequence fulfills the acceptance criteria with the ITL of 99/95, means that we are analyzing a successful sequence, i.e., a sequence that, with the only intervention of safety systems, meets the acceptance criteria in at least 95% of cases. In the case that the percentage of successful runs is lower than 99% we would have to classify the design as unacceptable. However, the “next class” is no longer a DBA class and the analysis requirements are different. Thus, for the purpose of checking fulfillment of acceptance criteria with ITL it is allowed to take into account other safety features additional to automatic safety systems, e.g., operator actions guided by emergency procedures. If those actions are effective to avoid exceedance of the acceptance criteria in a significant number of cases, the analysis of that sequence would be acceptable. The analysis of such a sequence gives acceptable results if the exclusive response of safety systems avoids exceeding the acceptance criteria in at least 95% of cases and if the combined response of safety systems and additional safety features avoids such exceedance in at least 99% of cases (always requiring a 95% confidence level).

Something similar occurs in the case of sequence reclassification into the next higher class due to its low probability of occurrence. Here, it can happen that the analyzed sequence is not successful, i.e., it does not fulfill the initial class acceptance criteria with STL or, in other words, by relying only on safety systems, the acceptance criteria are exceeded in more than 5% of cases. However, its probability is low enough as to reclassify it to the next class, i.e., to DEC-1. Then, the analysis of this sequence will give acceptable results if safety systems along with other safety provisions for DEC-1 are able to fulfill the acceptance criteria in at least 99% of cases.

In any of the above two cases, when this conclusion that “the design is not acceptable” comes from failure to fulfill DEC criteria, the design improvement should not necessarily apply to safety systems. The remedial actions, namely, improvement of performance, improvement of reliability and addition of a new level of protection, would apply to safety features for DEC.

From the above discussion it can be concluded that the E-BEPU methodology provides a natural way to implement the graded approach to safety analysis defined in IAEA SSR-2/1. The application of E-BEPU to DBA allows for identifying some DEC scenarios resulting from degradation of DBA conditions. In addition, it can be easily adapted to implement the analysis requirements for DEC. As a result, E-BEPU is an adequate methodology for any class of accident in the continuous analysis space composed by AOO, DBA and DEC. Specific analysis requirements and acceptance criteria can be used in each case.

The E-BEPU methodology does not only allow for identifying DEC scenarios derived from the analysis of DBA. In the context of the graded approach to safety analysis DBA and DEC are just different types of accident classes, each one with its own characteristics and E-BEPU provides enough flexibility as to apply it for both types of scenarios.

Another difference between design of safety features for DEC and design of safety systems is that the latter need to comply with much stronger regulatory requirements. Although some

requirements are being imposed for DEC, they do not have the same level of enforcement and uniformity among different countries. As a result, design and verification of safety systems is much more standard while design and verification of safety features for DEC is more flexible.

10 References

[1] International Atomic Energy Agency, Safety of nuclear power plants: Design, IAEA Safety Standards Series No.SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

[2] Dusic, M., Dutton, M., Glaeser, H., Herb, J., Hortal, J., Mendizábal, R., and 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, pp 63-77, 2014.

[3] Dusic, M., Hortal, J., Mendizabal, R.,Pelayo, F. NARSIS Deliverable 3.8 – Development and Description of E-BEPU Method – Part A “theoretical basis”, Vienna, 2019.

[4] Dusic, M., Hortal, J., Mendizabal, R.,Pelayo, F. NARSIS Deliverable 3.9 – Use of E-BEPU for Evaluation of Defence-in-depth, Vienna, 2019.