NARSIS

New Approach to Reactor Safety Improvements

WP5: Supporting Tool for Severe Accident Management

Del 5.5 – Use of the Extended Best Estimate plus Uncertainty (E-BEPU) method for SAMG

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:	Del 5.5 – Use of the Extended Best Estimate plus Uncertainty (E-BEPU) method for SAMG		
Month Due:	45	**Month delivered:**	40
Leading Partner:	GEN d.o.o.		
Version:	V1		

Primary Authors: Milorad DUSIC and Javier HORTAL (NUCCON GmbH)

Other contributors:

Deliverable Review:

- **Reviewer #1:** Ivica Basic & Ivan Vrbanic, APOSS **Date:** 06/12/2020
- **Reviewer #2:** Piotr Darnowski, WUT **Date:** 04/12/2020

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

1 Executive Summary 6

2 Introduction 7

3 SA scenarios as compared with DBA 8

4 Reference scenarios for the design of safety features for SA 9

5 Uncertainties in design verification 10

6 Design verification with E-BEPU in SA context 11

6.1 Applicable limits in SA 11

6.2 Time uncertainty in E-BEPU 12

6.3 Checking the simulation results 13

6.4 Tolerance levels in SA context. 13

7 An example of applicability of E-BEPU to SA 15

8 Additional considerations about sequence reclassification 17

9 Conclusion 18

10 References 19

List of Figures

Figure 1: Options for uncertain time management in E-BEPU. 12
Figure 2: Shapiro diagram for hydrogen-air-steam mixtures. 15

List of Abbreviations

BEPU	Best Estimate Plus Uncertainty
DBA	Design Basis Accident
DEC	Design Extension Condition
E-BEPU	Extended Best Estimate Plus Uncertainty Analysis
ITL	Increased Tolerance Level
LB LOCA	Large Break Loss Of Coolant Accident
LD	Level Of Defence
LOCA	Loss Of Coolant Accident
LOOP	Loss Of Off-Site Power
NRC	Nuclear Regulatory Commission
PAR	Passive Autocatalytic Recombines
PSA	Probabilistic Safety Assessment
SA	Severe Accidents
SAM	Severe Accident Management
SAMG	Severe Accident Management Guidelines
SBO	Station Blackout
STL	Standard Tolerance Level
TBS	Transition Break Size
TSC	Technical Support Centre
V&V	Verification And Validation

1 Executive Summary

The E-BEPU methodology [1] was developed as a tool for licensing analysis of Design Basis Accidents (DBA). Historically, these analyses have been performed using different approaches that, progressively, have taken advantage of phenomenological research, physical modeling and computer technology. From the highly conservative methodologies of the initial times of commercial nuclear energy, still being used to some extent, methodologies have evolved to more realistic modeling combined with consideration of analysis uncertainties. Nowadays, the most advanced methodologies that have been accepted by many regulators are the so-called Best-Estimate Plus Uncertainty (BEPU) where the use of realistic simulation models is combined with the analysis of uncertainties in model parameters or initial conditions of the analysis. The main feature of E-BEPU is to extend the scope of the uncertainty analysis typical of BEPU to include uncertainty in the configuration of the safety systems that are activated in the course of the accident.

The most evident differences between DBA and SA scenarios are related with phenomenology. From the point of view of an analysis methodology, different phenomena imply different simulation models but this does not necessarily implies different analysis procedures. However, there are other important points that could significantly impact analysis methodologies for Severe Accidents. For example, contrary to the case of DBA scenarios where protection essentially relies on automatic systems, the management of SA is mainly supported by human actions.

The application of E-BEPU implies the use of simulation codes that, especially in the case of severe accidents, may have a significant degree of complexity. When an analysis is performed that involves a reduced number of simulation runs it is feasible to manually check the simulation outputs looking for possible inconsistent results. However, when simulation is extensively used as in the case of E-BEPU, manual checks become inapplicable and it is recommendable to implement some automatic checking of the simulation outputs. This is especially important in the case of complex phenomenology, e.g., in severe accident conditions, where physical inconsistencies are more difficult to detect in an intuitive way.

Although the verification of the design of safety features provided for SAM is always a difficult task, E-BEPU allows for a feasible approach to such verification. It can provide additional insights that can be used for the development and V&V of SAMG, especially by identifying possible cliff-edge effects on one hand and by identifying very unlikely event sequences on the other hand that can be tolerated based on their unlikely occurrence, meaning that in some cases they can be treated as “practically eliminated”.

2 Introduction

The E-BEPU methodology [1] was developed as a tool for licensing analysis of Design Basis Accidents (DBA). Historically, these analyses have been performed using different approaches that, progressively, have taken advantage of phenomenological research, physical modeling and computer technology. From the highly conservative methodologies of the initial times of commercial nuclear energy, still being used to some extent, methodologies have evolved to more realistic modeling combined with consideration of analysis uncertainties. Nowadays, the most advanced methodologies that have been accepted by many regulators are the so-called Best-Estimate Plus Uncertainty (BEPU) where the use of realistic simulation models is combined with the analysis of uncertainties in model parameters or initial conditions of the analysis. The main feature of E-BEPU is to extend the scope of the uncertainty analysis typical of BEPU to include uncertainty in the configuration of the safety systems that are activated in the course of the accident.

When a safety system is initiated, its actual configuration is uncertain because there are possible failures that may occur with different probabilities. Characterizing these configurations requires, therefore, the use of a probabilistic model, in many aspects similar to those typical of PSA. By incorporating this type of models, E-BEPU is a methodology that integrates deterministic and probabilistic aspects. The use of tolerance levels to check compliance with regulatory limits is equivalent to limit the conditional exceedance probability of those limits, given the occurrence of the accident.

Although initially focused on the analysis of DBA, the applicability of E-BEPU goes beyond this scope. The effective integration of deterministic and probabilistic methods and the flexible use of different types of simulation and reliability models make E-BEPU an adequate methodological framework to verify the effectiveness of any system or protective feature designed to avoid exceeding some specified limits. In particular, the applicability of E-BEPU to assess safety features for control and mitigation of Severe Accidents (SA) is discussed below.

3 SA scenarios as compared with DBA

The most evident differences between DBA and SA scenarios are related with phenomenology. From the point of view of an analysis methodology, different phenomena imply different simulation models but this does not necessarily implies different analysis procedures. However, there are other important points that could significantly impact analysis methodologies for Severe Accidents. For example, contrary to the case of DBA scenarios where protection essentially relies on automatic systems, the management of SA is mainly supported by human actions.

Moreover, while a key assumption in DBA analysis is that only safety systems are trusted to perform safety functions, any available system, no matter its safety qualification, can be used to develop protective strategies under SA conditions. As a consequence, equipment reliability becomes an important variable since safety functions developed by qualified and redundant systems are more likely to get success than those performed by poorly qualified systems. There could be also some systems specifically designed for control and mitigation of severe accidents.

Both DBA and SA protection strategies need to take into account the plant state to perform adequate actions. In both cases, availability of reliable instrumentation, able to withstand accident conditions, is a need. In the case of DBA, the design of protection strategies requires to identify adequate safety variables and to determine as accurately as possible the conditions for the start-up of each safety system. From this point on, strategies are automatically applied when the plant state matches the identified conditions.

On the other hand, SA strategies need to take into account not only the state of physical processes as reported by the available instrumentation but also the state of plant systems, some of which may be degraded or unavailable as a consequence of the accident. This makes almost impossible to design SA strategies on the basis of well defined, prescriptive rules, as in the case of DBA. SA strategies are indeed developed in the form of Severe Accident Management Guides (SAMG) providing possible options and clues to the decision team in the Emergency Center.

Anyway, both the development of SA strategies and the design of automatic systems or DBA strategies, require defining an objective, to select one or more reference scenarios and to verify the adequacy and the effectiveness of the proposed actions in order to achieve that objective. Note that the term DBA actually refers to the design of safety systems, i.e., qualified automatic systems but any action, system or strategy needs to be designed on the basis of its own design objective and specified design scenarios. In this sense, the term “design basis scenario” can be used also referring to safety features (systems, actions, strategies) provided for SA.

4 Reference scenarios for the design of safety features for SA

The need to implement some safety feature for SA may result from different types of evidences identified either in real accidents, in SA research studies or in safety assessments, in particular level 2 PSA. Actually, when developing a level 2 PSA, the accident progression is modeled on the basis of existing knowledge on phenomenology, system performance and expected environmental conditions, most often derived from real accidents or SA research. For this reason, level 2 PSA will be a main source of information for analysts trying to develop safety features provided for SA or to assess the effectiveness of those features.

The first step in the design of a safety feature provided to cope with the effects of severe accidents is to define the design objective, i.e., the effects that the designed feature should produce or those that should be avoided. Most often, the use of a particular safety feature is only necessary or advisable in specific types of accident scenarios that should be delimited as well. One or more of these scenarios will then be selected as a reference to determine the design basis for the new safety feature.

It is advisable to reduce as much as possible the number of reference scenarios for a given feature and, whenever possible, this number should be reduced to one. If a level 2 PSA exists for the same plant or for the same design concept for which the safety feature is being designed, the task of determining the reference scenario can be remarkably easier. Level 2 PSA scenarios are grouped by bins, each bin containing scenarios with similar characteristics from the point of view of accident progression. In the process of determining a reference scenario for a safety feature, identifying the PSA bins where such safety feature may provide a benefit would be the first screening step.

When a level 2 PSA is not available it could be necessary to initiate the screening process from scratch. Most likely, this process will start with a binning task resulting in a reduced number of bins, not necessarily the same of the level 2 PSA, but equally useful to screen-out those bins where the safety feature of interest is of lower relevance. No matter the type of binning being used, after the initial screening each remaining bin shall be analyzed in more detail in order to determine the most limiting case from the point of view of the effectiveness of the safety feature. Inter-bin comparisons shall also be performed in order to select the final reference scenario.

Finding a single reference scenario for the design of a safety feature is not always possible. SA scenarios often involve a high level of complexity and there could be aspects or phases of a given scenario where the same safety feature could be beneficial or harmful or where its effectiveness could greatly vary. As above indicated, when a single reference scenario is difficult to find, it would be necessary to use multiple reference scenarios but reducing the number of such scenarios is of paramount importance to increase the feasibility of the design and verification process.

The strategy here described to find reference scenarios is not new. Similar strategies are used for many types of analysis, not necessarily restricted to the field of severe accidents. Actually, the process to define design basis transients or accidents for safety systems is in many aspects similar. Another example of the same type of strategy applied to the selection of simulation cases for assessment of SAMG actions and strategies is given in [2].

Once the reference scenario has been selected, the safety feature will be designed with enough capability to achieve the intended objectives in that scenario. In general those objectives consist of preventing some specified limits from being reached. It is assumed that if the safety feature is able to fulfill its goals in the reference scenario, the same goals will be fulfilled in less limiting scenarios. The design process will depend very much on the specific characteristics of the safety feature and it falls out of the scope of this report.

After completing the design, the capability of the safety feature should be verified. In the case of safety features for SA, as in the case of safety systems for DBA, the possibility to perform an experimental verification is very limited and the use of analytical techniques is inevitable. To this purpose, the E-BEPU methodology may provide valuable support.

5 Uncertainties in design verification

The verification process is not only necessary to confirm that the designed safety feature performs as expected under the conditions defined by the design assumptions. Other aspects like robustness of the design upon system failures, variation in the assumed conditions or additional perturbations should also be ascertained.

One of the difficulties for sound design verification is the level of uncertainty associated to SA scenarios. Uncertainty is always inherently linked to the verification of any safety design but the nature and the magnitude of the uncertainties may greatly vary from case to case. This is a main difference between the verification of safety systems for DBA and safety features for SA. The main uncertainties associated to the analysis of DBA are those related with model parameters that cannot be precisely determined and safety system configurations that may vary due to system failures. BEPU methodologies used in the analysis of DBA typically address parametric uncertainties in an analytic manner while system configurations are specified by using bounding assumptions like the single failure criterion. The E-BEPU methodology, as proposed in [1], applies analytical methods to both types of uncertainties.

In the analysis of SA scenarios for verification purposes, those uncertainties are also present but there are new and very important uncertainties associated to new types of phenomena that need to be considered in SA analysis. On the one hand, stochastic phenomena may appear that are not credited in DBA. On the other, human actions play an essential role in safety management under SA conditions. Both types of events have a common characteristic, namely, that their occurrence time is uncertain.

Events considered in DBA analysis are almost exclusively limited to initiation of safety systems, in most cases automatically triggered when the corresponding set-point is reached. This means that the occurrence times of the events is not uncertain but determined by plant processes except for the effects, usually negligible, of small delays in instrumentation response or signal processing. In the very few cases that operator actions are credited in DBA, the uncertainty in the operator action time is solved by demonstrating that no safety limit is exceeded if the operator delay is lower than a pre-established maximum value. Therefore, the time uncertainty is not explicitly analyzed.

The situation is totally different in SA. The great majority of the events considered in the analysis of SA sequences occur at uncertain times. Stochastic phenomena are, by definition, physical processes of uncertain occurrence. In most cases, the phenomenon may not occur unless the plant state matches some conditions but, even if those conditions are met, the phenomenon may or may not occur. A typical example of stochastic phenomenon under SA conditions is hydrogen burn-up. Violent hydrogen combustion may only occur if concentrations of hydrogen, air and steam match the so-called flammability conditions. However, matching those conditions does not imply burn-up initiation. An ignition source is additionally needed and, therefore, the flammability conditions could even vanish without actual initiation of the hydrogen combustion.

Operator actions are a particular case of unpredictable events. Taking apart the particularly complex case of errors of commission, operators act under the guidance of procedures or SAMG, in the latter case with the intervention of the Technical Support Center (TSC). When following procedures or when using SAMG to take decisions, the time when the operator is asked to do something is already uncertain. In addition, executing the action may take some time, difficult to predict. It could even happen that a demanded action is skipped by the operator, especially under the high stress conditions imposed by the accident. Delays of operator actions in SA conditions can be significantly long because they include communications between the control room and the TSC and the decision time of TSC members in addition to the usual delay related to operator performance. The importance of time uncertainty in safety issues is clear. A protective action taken too late could be inefficient and therefore equivalent to a failure or it could even have a worsening effect. It is well known (see, for example the conclusions of [3]) that time uncertainty may dominate over other types of uncertainty and therefore it cannot be neglected.

6 Design verification with E-BEPU in SA context

Usual BEPU methodologies for design verification in a DBA environment are difficult to apply in SA, especially because of the time uncertainty issue. Most BEPU methodologies used for DBA are based on a probabilistic approach to uncertainty and assign a probability distribution to each uncertain parameter. Those probability distributions are assumed independent of each other and they are sampled to obtain random values of the parameters which are then used to perform simulation runs. This approach also assumes that the distribution probability of each parameter is independent of the plant state and therefore, it is known before the simulation and remains unchanged during the simulation run.

When uncertain time delays are present these assumptions are not always valid. The actual delay of an event may influence the delays of subsequent events. Also, time delays may strongly depend on the plant state. An example of the latter are delays of operator actions which can be greatly influenced by the dynamic conditions of the plant and the number of concurrent operations they should perform at a given moment in the accident evolution.

Another point to discuss when moving from DBA to SA is system configurations due to the difference in mission time that the analysis of each class of accident requires. In DBA it is assumed that a system or system train is either working or failed from the beginning and it remains in the same state along the accident. This is a reasonable assumption in DBA because, by definition, the design conditions are maintained in the course of the accident. Instead, in a severe accident, where longer mission times are used for the analysis and plant conditions could become quite aggressive for the integrity of plant systems, system failures are more likely to occur while in operation. This type of failures is another particular case of stochastic event with probability highly dependent on the plant state.

All these difficulties can be adequately addressed by E-BEPU. Stochastic events can be modeled in the E-BEPU event trees and the probability calculations may include dependencies on plant state when known.

6.1 Applicable limits in SA

Acceptance criteria required by the regulator are well defined for DBA. However, in the case of protection against SA, the licensing requirements are not equally strict. Although Design Extension Conditions (DEC), including SA, are receiving increased regulatory attention, criteria are not defined with the same level of precision nor they have the same level of enforcement.

Nevertheless, assessing the adequacy and effectiveness of safety features in not only important for licensing purposes. Design verification is the last step of the design process and it is needed even if not required by regulators. Applicable limits and acceptance criteria must be consistent with the characteristics of the reference scenarios and there is a growing consensus on the type of limits that should be used for plant states beyond the traditional DBA scenarios.

An example of proposed limits for the whole range of plant states can be found in [4] (App 2) where a Level of Defence (LD) is proposed for each type of plant state. For lower plant states (LD 1 to 3a), the proposed limits are coincident with the regulatory limits used worldwide. For higher plant states, the proposed limits are widely accepted although they cannot be considered regulatory limits. For the specific case of SA sequences, which are classified as DEC-2 in [5], the proposed limits are those of LD 4, i.e., maintaining the containment integrity and avoiding the need for emergency countermeasures except for those that are of limited scope in terms of area and time.

Note that LD 5 in App 2 of [4] is not defined in terms of limits to be maintained. It rather indicates that all the established limits have been exceeded because this LD corresponds to plant states beyond the scope of any class of safety design.

6.2 Time uncertainty in E-BEPU

As already indicated, one of the main distinctive features of E-BEPU with respect to usual BEPU methodologies is the consideration of uncertainty in system configurations. Without discussing the reasons for the difference, it should be noted that this type of uncertainty is not treated as a simple extension of the scope of BEPU uncertainties. While the analysis of typical parametric uncertainties is based on random sampling methods, system configurations give rise to an event tree model which implements a systematic scanning of all possible configurations.

Uncertain occurrence times are, like most uncertain model parameters, continuous random variables. From this point of view, they are candidates for a random sampling approach. However, given the importance of time uncertainty, it could be convenient to retain low probability time values that could be lost when applying random sampling. This can be achieved if systematic scanning methods are used for time uncertainty. In both cases, it is important to recall that probabilities of stochastic events may depend on the plant state and, in general, they are unknown before the simulation. If random sampling is applied to uncertain times, the simulation should run until the stochastic event becomes possible, then the random occurrence time is chosen taking into account all the possible dependencies on plant conditions. If systematic scanning is applied, the probability of each time value is also calculated in accordance with the plant conditions given by the simulation. Both options are possible in E-BEPU as illustrated in Figure 1.

The random sampling option is represented in Figure 1.a where a single child branch is generated from the parent sequence for a particular stochastic event. The event probability is split in two factors, one for the total occurrence probability, i.e. the probability that the event occurs at any time, the other for the actual occurrence time. The former is a single probability value which is assigned to the child branch and its complement is assigned to the continuation of the parent sequence. The latter is a continuous random variable which is sampled to obtain an aleatory value of the occurrence time.

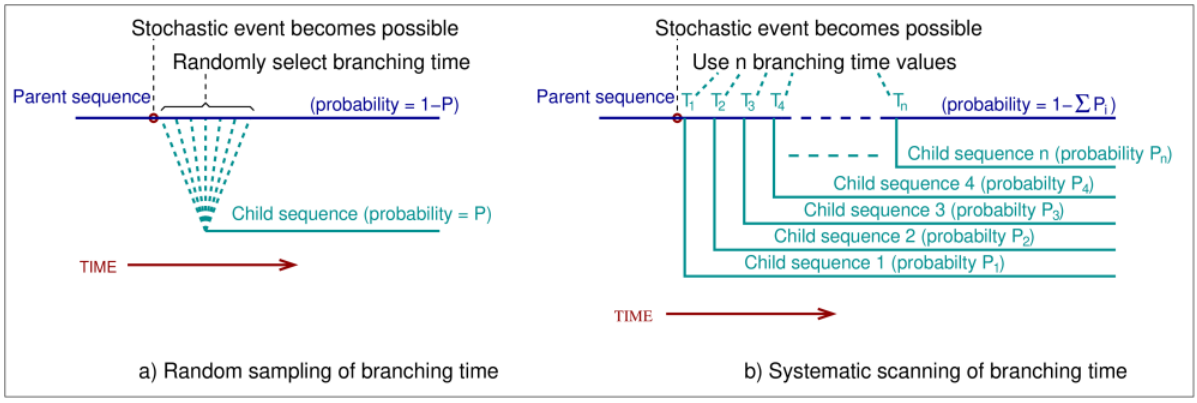

Figure 1: Options for uncertain time management in E-BEPU.

Systematic scanning is represented in Figure 1.b. Given a particular sequence in the event tree, when a stochastic event becomes possible, several child sequences are derived from the parent sequence, all of them due to the occurrence of the same event and differing only in the occurrence time. Being the occurrence time a continuous random variable, it is discretized to obtain a manageable number of time values, each one with a probability calculated from the continuous probability distribution. Each child branch corresponds to one of the selected time values whose probability is assigned to the child branch. The total conditional probability of the child sequences plus the conditional probability of the remaining of the parent sequence must sum-up to 1.

Probability distributions are not always easy to manage when dynamic dependencies are present. An alternative description of the randomness of the occurrence time is given by

occurrence rates. The occurrence rate is the occurrence probability per unit time in a differential time interval. Dynamic dependencies are much easier to formulate in terms of occurrence rates than in terms of probability distributions. Nevertheless, all the above discussion applies also when using occurrence rates if the following relationships between occurrence rates and probability distributions are taken into account:

$$F(t) = \int_0^t f(\tau)d\tau \quad ; \quad 1 - F(t) = exp\left(-\int_0^t \lambda(\tau)d\tau\right) \quad ; \quad f(t) = \lambda(t)\big(1 - F(t)\big)$$

where λ(t) is the occurrence rate, f(t) is the probability density function (pdf), and F(t) stands for the cumulative distribution function (cdf). More on this subject can be found in https://www.wiley.com/en-us/Risk+and+Safety+Analysis+of+Nuclear+Systems-p-9780470907566.

6.3 Checking the simulation results

The application of E-BEPU implies the use of simulation codes that, especially in the case of severe accidents, may have a significant degree of complexity. It is well known that sometimes the results of a simulation code may not reflect the real behavior of the simulated system, even if the code has been validated and the implemented model is considered adequate. This may occur, among other reasons, when the physic process evolves beyond the intended scope of the code equations, when the numerical algorithm goes outside its validity range or when the values of some parameters or combinations thereof are inconsistent with the assumptions of the model equations.

In some cases these conditions are detected by the code itself and the simulation crashes. However, in complex codes it is difficult to foresee all the possible inconsistencies and it may occur that the simulation produces some results apparently correct but physically inconsistent. Some of these mechanisms are behind the so-called user effect that results in different code outputs depending on the specific values that different users provide for the code input parameters. Qualified users are, of course, less exposed to the risk of getting inconsistent output results, but they are not immunized at all.

When an analysis is performed that involves a reduced number of simulation runs it is feasible to manually check the simulation outputs looking for possible inconsistent results. However, when simulation is extensively used as in the case of E-BEPU, manual checks become inapplicable and it is recommendable to implement some automatic checking of the simulation outputs. This is especially important in the case of complex phenomenology, e.g., in severe accident conditions, where physical inconsistencies are more difficult to detect in an intuitive way. Simulation models can be of higher or lower quality and, therefore, their results can be more or less representative of reality but it is important, at least, to ensure that the code outputs are consistent with the model equations.

A continuous post-processing of simulation outputs can be adequate for this purpose. As proposed in [6], the model equations can be used to obtain relationships between the output variables, different from those implemented in the code. An external code, running in parallel with the simulation code, could continuously check whether the code outputs comply with these relationships, raising an alarm when some inconsistency is detected.

6.4 Tolerance levels in SA context.

Tolerance levels are used in E-BEPU, like in conventional BEPU, to determine whether the design of a safety feature is acceptable or not. An important improvement with respect to BEPU is that two tolerance levels are used in E-BEPU, namely the Standard Tolerance Level (STL), similar to the usual BEPU tolerance level and the Increased Tolerance Level (ITL). As explained with more detail in [1], the ITL provides a higher level of Defence-In-Depth and helps to detect cliff-edge effects.

In DBA analysis, the typical value of STL is 95/95 as in the case of BEPU. This tolerance level applies to the limits of the class where the analyzed accident is classified. The ITL value proposed in [1] was 99/95, i.e., 99% coverage probability with 95% confidence level, applicable to the limits of the next higher class of the accident.

The application of E-BEPU in an SA environment requires some more discussion about tolerance levels. First, it must be noted that severe accidents belong to the so-called DEC-2 class of accident conditions [5] which is the last class and this makes inapplicable the E-BEPU requirement to comply with the limits of the "next higher class" with ITL. In addition, the higher level of uncertainty in SA scenarios with respect to DBA, makes it difficult to maintain the same STL for compliance with the defined acceptance criteria. However, the philosophy of graded approach to safety allows for a less stringent tolerance level in higher severity classes.

The STL value used for SA scenarios should be such that the frequency of sequences that could result in an overpass of the defined acceptance criteria make them fall into the category of "practically eliminated" using the terminology of [5]. Lack of experience in the application of E-BEPU to SA makes inadvisable to define a precise STL. Tentative values around 90/90 could be used as an initial guess.

7 An example of applicability of E-BEPU to SA

Hydrogen control is a key issue in SA scenarios since hydrogen production is a characteristic process of severe accidents and the uncontrolled combustion of hydrogen may be an important challenge for containment integrity. During the in-vessel phase of the accident, hydrogen generated in the reactor core is released to the containment through pipe breaks if they exist or through relief and safety valves if the reactor coolant system is still maintaining its integrity. When the reactor pressure vessel fails and the corium is poured on the containment floor, the corium-concrete interaction generates additional amounts of hydrogen and also carbon monoxide, another combustible gas. The resulting concentration of hydrogen in the containment atmosphere depends on the physic-chemical conditions and also on the containment geometry.

The composition of the containment atmosphere during a severe accident may be quite complex but, from the point of view of hydrogen combustion, it can be considered as a mixture of three main components, namely, air, steam and hydrogen. Depending on the relative concentrations of these components hydrogen combustion may occur or not and, when occurring, there are several possible combustion regimes. In addition, an ignition source is usually needed to initiate the combustion process. These and other conditioning factors make very difficult to predict when hydrogen combustion will occur in the course of a severe accident.

A simplified approach to the analysis of hydrogen combustion hazard is to use the well-known Shapiro diagram (Figure 2) to determine when the containment atmosphere becomes flammable and which regime of flame propagation speed can be expected, including the transition to detonation regime (red area in Figure 2). Once the flammability conditions have been reached, actual combustion will only occur upon activation of an ignition source. The difficulty to track all the possible ignition sources makes recommendable to consider hydrogen ignition as a stochastic phenomenon that may occur at an uncertain time while the flammability conditions exist. In addition, the pressure peak hitting the containment as a consequence of the combustion can be considered as an uncertain variable. The analysis should be performed for those containment volumes where hydrogen may concentrate and the flammability conditions are more likely reached.

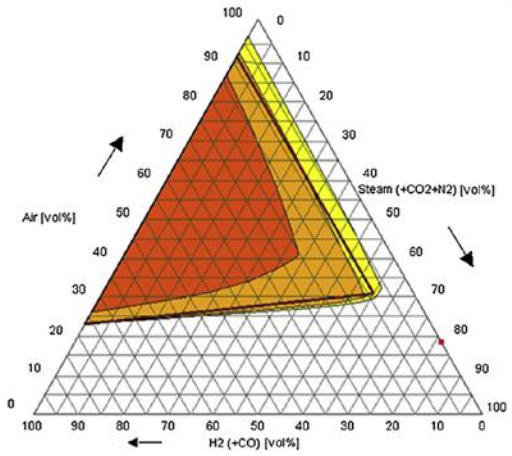

Figure 2: Shapiro diagram for hydrogen-air-steam mixtures.

An efficient way to maintain the hydrogen concentration as low as possible is the use of PAR. These devices stimulate the hydrogen oxidation at concentrations well below the flammability limit. If a sufficient number of PAR is available, the flammability conditions would not be reached and the risk of containment failure due to hydrogen deflagration or detonation is minimized. Determining the number, position and capacity of the devices to be installed are the main design issues of a PAR system. To this aim, the most limiting scenarios need to be identified since they will provide the design basis for the PAR system.

However, hydrogen releases to the containment may greatly vary in location and intensity depending on the specific accident scenario and the optimal configuration of PAR may vary

from case to case. Therefore, the final PAR configuration should be an envelope of the optimal configurations resulting from the most limiting scenarios and, most likely, the design verification should be performed for two or more reference scenarios.

An additional problem for hydrogen control is that the hydrogen distribution in the containment atmosphere is not uniform and flammability conditions can be reached in a particular region while maintaining a low average concentration in the whole containment. As a consequence, a more or less detailed 3D model of the containment is necessary in order to identify hydrogen paths and accumulation areas both for design and verification purposes.

Once the design of a PAR system is completed, it can be verified by using the E-BEPU methodology. The first step is to identify the reference scenarios. As above indicated, hydrogen releases to containment may take place through pipe breaks or through relief or safety valves with different resulting hydrogen distributions. Two typical SA scenarios for hydrogen control verification are those initiated from a Large-break LOCA (LB-LOCA) or from a SBO.

As indicated in section 6.1, the applicable limits for SA scenarios would be maintenance of the containment integrity and avoidance of emergency countermeasures. However, the design of the PAR system is specifically intended to avoid phenomena that could impair the containment integrity and this will be the limit that needs to be analyzed in the verification process. This limit can be reformulated in terms of maximum acceptable pressure peak in order to make the application of tolerance levels easier. Using the deflagration or detonation limit as a surrogate for containment integrity could be acceptable if sufficient justification is provided. However, it has to be recalled that hydrogen burn-up is not the only mechanism for containment failure in LB-LOCA or SBO scenarios and that all of them need to be taken into account to evaluate the eventuality of a containment failure. Compliance with the containment integrity limit is required with STL while the use of ITL for the next class limits is not applicable to SA scenarios as indicated in section 6.4.

For the development of E-BEPU event trees the following considerations apply. Both LB-LOCA and SBO are scenarios where not only PAR are relevant. There are other safety features that need to be taken into account for the control of the accident. In particular, containment spray and fan coolers may influence the atmospheric conditions of the containment and, therefore, the hydrogen flammability. Safety systems designed for reactor coolant protection, especially injection systems, are relevant to control the hydrogen generation while containment safeguards such as spray or fan coolers are relevant to control the hydrogen distribution and flammability. All these systems need to be taken into account for the deployment of the E-BEPU event trees.

Severe Accident Management strategies, as defined in the corresponding guides, are also relevant. To this regard, operation of the containment spray can be especially important because of the well-known effect of containment deinertization if it is operated under high hydrogen concentration conditions.

Uncertainties that need to be considered in the E-BEPU analysis are not limited to those related to simulation model parameters, typically considered in a BEPU analysis. An important uncertainty related to hydrogen combustion is the resulting pressure peak that is very much dependent on the combustion regime and the resulting flame propagation velocity. The number and location of PAR actually working, as in the case of any other safety system, should be reflected in the E-BEPU event tree structure. There are also several important time uncertainties. For example, as above indicated, if PAR are unable to avoid flammable conditions, the ignition time is uncertain. Also, initiations of containment systems, when required by SAMG, are human actions with associated time uncertainty.

Once the E-BEPU event tree has been developed taking into account the above considerations, the objective of the analysis is to verify that the containment pressure remains below the failure limit with STL for any sequence that cannot be reclassified. The reclassification criterion should be such that reclassified sequences will fall into the category of practically eliminated sequences due to their very low frequency.

8 Additional considerations about sequence reclassification

One of the distinctive features of E-BEPU is the possibility to reclassify sequences with low enough likelihood of occurrence. This feature, which can be of interest for the development and V&V of SAMG, was already explored in [1] where it was shown that the methodology was well suited to deal with the NRC proposal for the introduction of the so-called transition break size (TBS) for the LB LOCAs. Within this approach, the NRC proposed to divide LB LOCAs into two categories; below TBS and above TBS with the requirement that LB LOCAs in the category above the TBS are at least 100 times less likely to occur compared with the likelihood of occurrence of LB LOCAs classified in the category below TBS.

For LB LOCAs below the TBS, the requirements, tolerance level and acceptance criteria would remain the same as in current regulations. However, for LB LOCAs above TBS, although the acceptance criteria would remain unchanged, some analysis requirements like assuming loss of off-site power (LOOP) or additional single failure would be removed. Crediting some non-safety equipment would also be possible for LOCAs in this category.

When applying E-BEPU to LB LOCA below TBS, sequences with additional equipment failures or LOOP would be likely enough as for not being reclassified, so compliance with acceptance criteria at STL would be required for those sequences as usual. For LB LOCAs above TBS, it would however be possible that sequences with additional failures or LOOP were not compliant with the acceptance criteria. By following the right hand side of the E-BEPU flow diagram (please see [1] or other NARSIS deliverables) these sequences would have so low probabilities of occurrence (at least two orders of magnitude lower than in the case of LOCA below TBS) that they could be reclassified into the next category. However, as there is no higher class of DBA and no acceptance criteria to be violated, they can be treated as being in the “residual category”. This approach is fully consistent with the NRC rulemaking proposal.

LB-LOCA below and above TBS can be treated in E-BEPU as a special case of two different categories with the same acceptance criteria and different analysis requirements. For LOCAs below the TBS, following the E-BEPU procedure, it has to be shown that they fulfill the acceptance criteria with the STL for their category AND in addition that they fulfill the acceptance criteria of the next class with the ITL. In this special case, this means that, using the relaxed analysis requirements of the higher category, they must fulfill the same acceptance criteria with ITL. Even though the acceptance criteria are the same, by requiring higher level of compliance with lower analysis restrictions helps minimizing cliff-edge effects. The benefit of the use of two tolerance levels is therefore maintained as in the general case of E-BEPU.

In this way, E-BEPU imposes additional acceptance criteria for LB LOCAs below the TBS and gives relaxation to LB LOCAs above the TBS, which have at least 100 times less probability of occurrence then those below the TBS.

Using E-BEPU approach can in this way be beneficial for the development and V&V of SMAG as insights on cliff-edge effects minimization and likelihood of large LB LOCAs can be adequately taken into account.

9 Conclusion

When discussing the applicable limits for SA, for the specific case of SA sequences, which are classified as DEC-2, the proposed limits are maintaining the containment integrity and avoiding the need for emergency countermeasures except for those that are of limited scope in terms of area and time. For this purpose, E-BEPU cannot at the moment offer more than what is achieved by other, established types of safety analysis. However, when addressing time uncertainties which are quite large in SA, the E-BEPU can address them in a systematic manner. Uncertain occurrence times are, like most uncertain model parameters, continuous random variables. From this point of view, they are candidates for a random sampling approach. However, given the importance of time uncertainty in SA, it could be convenient to retain low probability time values that could be lost when applying random sampling. This can be achieved if systematic scanning methods are used for time uncertainty. If random sampling is applied to uncertain times, the simulation should run until the stochastic event becomes possible, then the random occurrence time is chosen taking into account all the possible dependencies on plant conditions. If systematic scanning is applied, the probability of each time value is also calculated in accordance with the plant conditions given by the simulation. Both options are possible in E-BEPU.

The application of E-BEPU implies the use of simulation codes that, especially in the case of severe accidents, may have a significant degree of complexity. When an analysis is performed that involves a reduced number of simulation runs it is feasible to manually check the simulation outputs looking for possible inconsistent results. However, when simulation is extensively used as in the case of E-BEPU, manual checks become inapplicable and it is recommendable to implement some automatic checking of the simulation outputs. This is especially important in the case of complex phenomenology, e.g., in severe accident conditions, where physical inconsistencies are more difficult to detect in an intuitive way.

Although the verification of the design of safety features provided for SAM is always a difficult task, E-BEPU allows for a feasible approach to such verification. It can provide additional insights that can be used for the development and V&V of SAMG, especially by identifying possible cliff-edge effects on one hand and by identifying very unlikely event sequences on the other hand that can be tolerated based on their unlikely occurrence, meaning that in some cases they can be treated as “practically eliminated”.

10 References

1. 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, Oct. 2014.

2. NEA/OECD Committee on the Safety of Nuclear Installations, Informing Severe Accident Management Guidance and Actions for Nuclear Power Plants through Analytical Simulation. NEA/CSNI/R(2017)16. https://www.oecd-nea.org/jcms/pl_19820

3. NEA/OECD Committee on the Safety of Nuclear Installations,Safety Margin Evaluation - SMAP Framework Assessment and Application - Final Report. NEA/CSNI/R(2011)3. http://www.oecd-nea.org/nsd/docs/2011/csni-r2011-3.pdf

4. INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants. IAEA-TECDOC-1791, Vienna, 2016. https://www-pub.iaea.org/MTCD/Publications/PDF/TE-1791_web.pdf

5. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of NUCLEAR POWER PLANTS: Design, IAEA Safety Standards Series No.SSR-2/1 (Rev. 1), IAEA, Vienna 2016. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1715web-46541668.pdf

6. Herrero Santos, R., Izquierdo Rocha, J.M., “Development of a Computer Tool for In-Depth Analysis and Post Processing of the RELAP5 Thermal Hydraulic Code”, NUREG/IA-0253, U.S. Nuclear Regulatory Commission, April 2011. http://pbadupws.nrc.gov/docs/ML1111/ML11118A088.pdf.