RISK-INFORMED REGULATION: HANDLING UNCERTAINTY FOR A RATIONAL MANAGEMENT OF SAFETY

ENRICO ZIO
Dept. of Energy, Polytechnic of Milan
Via Ponzio 34/3, I-20133 Milan, Italy
E-mail : enrico.zio@polimi.it

Received July 14, 2008

A risk-informed regulatory approach implies that risk insights be used as supplement of deterministic information for safety decision-making purposes. In this view, the use of risk assessment techniques is expected to lead to improved safety and a more rational allocation of the limited resources available. On the other hand, it is recognized that uncertainties affect both the deterministic safety analyses and the risk assessments. In order for the risk-informed decision making process to be effective, the adequate representation and treatment of such uncertainties is mandatory.

In this paper, the risk-informed regulatory framework is considered under the focus of the uncertainty issue. Traditionally, probability theory has provided the language and mathematics for the representation and treatment of uncertainty. More recently, other mathematical structures have been introduced. In particular, the Dempster-Shafer theory of evidence is here illustrated as a generalized framework encompassing probability theory and possibility theory. The special case of probability theory is only addressed as term of comparison, given that it is a well known subject. On the other hand, the special case of possibility theory is amply illustrated. An example of the combination of probability and possibility for treating the uncertainty in the parameters of an event tree is illustrated.

KEYWORDS : Risk-Informed, Nuclear Power Plant, Uncertainty, Epistemic, Aleatory, Probability, Dempster-Shafer Theory, Possibility, Monte Carlo, Event Tree.

1. REGULATING THE RISK FROM A NUCLEAR POWER PLANT

Classically, the control of the risk associated to the operation of a nuclear power plant has been founded on the definition of a group of events representing credible *worst-case* accident scenarios (the so-called *Design Basis Accidents, DBAs*) and on the prediction and analysis of their consequences by deterministic calculations. Then, the safety and protection of the system is designed against such events, to prevent them and to protect from, and mitigate their associated consequences. This traditional approach to regulating nuclear safety by the verification that a nuclear plant can withstand a set of prescribed accident scenarios judged as most adverse, conjectures that if a plant can cope with the DBAs, it will also be capable of handling any other accident.

In this view to safety, the underlying concept for protecting a nuclear power plant is the so called *defense-in-depth* which has become the design philosophy for attaining acceptable levels of safety. This *structuralist defense-in-depth* viewpoint and the safety margins derived from it, have been embedded into conservative regulations aimed at enveloping all credible accidents, for what concerns the challenges and stresses posed on the system and its protections. In fact, such view to nuclear safety has been embraced into a number of design and operating regulatory requirements, including [1]: i) the use of redundant active and/or passive engineered safety systems, to avoid the risks from single failures; ii) the use of large design safety margins to cope with the uncertainty in the actual response of the safety systems under accident conditions; iii) the demand of quality assurance practices on materials, manufacturing and construction; iv) the restriction of system operation within predetermined bounds; v) the definition of requirements for the testing, inspection and maintenance of the structures, systems and components to guarantee the desired safety levels.

The approach to safety above illustrated has been regarded effective in providing a conservative means for managing the uncertainties in the system behaviour and its modelling within the safety analyses. However, it is widely recognized that the reliance on purely deterministic analyses for the verification of nuclear safety may not be rational nor sufficient for bounding the required high levels of safety across all potential accident events and protective safety systems [2]. On one side, the practice of referring to DBAs may lead to the consideration of excessively conservative scenarios, but also highly unlikely, with a penalization of the industry due to the imposition of unnecessarily stringent regulatory burdens on the protective barriers for defense-in-depth. On the other hand, the conjecture that protecting from DBAs would give reasonable assurance of protecting from any accident has been proven wrong, e.g. by the occurrence of the Three Mile Island accident in 1979.

The above considerations have led to the arising of the *Probabilistic Risk Assessment (PRA)* approach for nuclear safety, based on the inclusion into the analysis of the likelihood of all potential accident scenarios by considering the reliability of the protection systems through the introduction of probabilistic measures for the treatment of the uncertainty in their behaviour [3-5]. This allows addressing some of the shortcomings of the DBAs thanks to a systematic modelling of more realistic scenarios, including multiple failure events (the so-called *Beyond Design Basis Accidents, BDBAs*) and to the definition of the level of risk from the plant in quantitative terms, [1-2]. Furthermore, the PRA analysis can be used to prioritize improvements in the design and operation of the plant for greatest risk reduction. On the other hand, it is impossible to guarantee that PRA captures all the accident events and scenarios contributing to risk and its quantitative results may be affected by very large uncertainties which make difficult their direct use for decision making.

Today's trend in the control of nuclear safety is drifting towards an integrated decision making process that combines the insights from the deterministic and probabilistic analyses with the regulatory requirements and cost-benefit considerations. This approach is increasingly adopted for a more efficient use of resources for increased safety and reduced regulatory burden in the application of a *rationalist* defense-in-depth philosophy. Since according to this approach risk information is to be used as adjunct to the deterministic and prescriptive body of regulations, it is often termed *risk-informed*, to unambiguously differentiate it from the *risk-based* approach based solely on insights from a PRA.

The risk-informed approach aims at systematically integrating deterministic and probabilistic results to obtain a rational decision on the utilization of resources for safety. In such rationalization, explicit consideration is given to the likelihood of events and to their potential consequences.

The undertaking of this approach has led to a number of efforts of risk-informing of existing regulations, i.e. rationalizing regulatory requirements by risk information. This has meant in particular the possibility of allowing changes in safety requirements upon demonstration that the corresponding change in the risk from the plant is acceptably small and still within the design bounds [6], [7-9]. Several instances of these efforts have demonstrated the effectiveness of the approach, perhaps the best still being the application in practice of the maintenance rule which has provided a foundation for making risk insights and prioritization of use in day to day operations [10].

2. UNCERTAINTY

Uncertainty is an unavoidable component affecting the behavior and modeling of systems. In spite of how much dedicated effort is put into improving the understanding of systems, components and processes through the collection of representative data, it is not realistic to think that uncertainty will be ever eliminated completely from the analysis and modeling of the behavior of complex systems.

Henceforth, the appropriate characterization, representation, propagation and interpretation of uncertainty are fundamental issues to be addressed for benefiting from a risk-informed approach to nuclear safety.

Indeed, it is recognized that uncertainties affect the models, computer codes and data used to quantitatively represent and reproduce the evolution of the nuclear processes and the response of the nuclear systems in operational and accidental conditions. The capability of structures, systems and components to withstand accidental events is also not fully characterized. Within the current trend of using best estimate codes for deterministic accident analysis, the control of such uncertainties entails the combination of a *reasonably conservative* selection of the input and parameter data with the propagation of the associated uncertainties onto the analysis outcomes. The expected end result is the demonstration of reasonable assurance on the availability of adequate safety margins, with a high level of confidence that failure event conditions are avoided [2].

On the other hand, uncertainty is a major issue of concern also in PRA, due to both the inherent stochastic character of the failure processes and to the incomplete knowledge of the analysts on such processes. This gives rise to uncertainty in [2]: i) the parameters used in the quantification of the PRA model, e.g. the failure event frequencies, component failure and human error probabilities; ii) the assumptions undertaken in the analysis and models used, e.g. for representing common cause failure events, the influence of the human operators and organizational procedures; the completeness of the analysis, i.e. the inclusion of all risk-contributing events and all factors influencing the risk from a nuclear power plant, e.g. ageing and organizational effects.

In order for the integrated, risk-informed decision making process to virtuously benefiting from the combination of the systematic deterministic and probabilistic analyses of the safety of a nuclear power plant, it is necessary that an adequate representation and treatment of the related uncertainties be provided.

The uncertainty can be considered essentially of two different types: i) randomness due to inherent variability in the system behavior and ii) imprecision due to lack of knowledge and information on the system. The former type of uncertainty is often referred to as objective, aleatory, stochastic whereas the latter is often referred to as subjective, epistemic, state-of-knowledge [11-12].

It is recognized that the distinction between aleatory and epistemic uncertainty plays an important role in the risk assessment framework applied to complex engineered systems such as the nuclear power plants. In the context of risk analysis, the aleatory uncertainty is related to the occurrence of the events which define the various possible accident scenarios whereas epistemic uncertainty arises from a lack of knowledge of fixed but poorly known parameter values entering the evaluation of the probabilities and consequences of the accident scenarios [12].

In current risk practice, both types of uncertainties are represented by means of probability distributions. However, resorting to a probabilistic representation of epistemic uncertainty may not be possible when sufficient quantitative data is not available for statistical analysis, even if one adopts expert elicitation procedures to incorporate diffuse information into the corresponding probability distributions, within a subjective view of probability. Indeed, an expert may not have sufficiently refined knowledge or opinion to characterize the relevant epistemic uncertainty in terms of probability distributions [12-15].

For instance, when there is no information to support a clear-cut decision out of a number of credible alternatives, a uniform probability distribution is typically used to characterize epistemic uncertainty. Considering an uncertain variable $x \in [a,b]$, the uniform distribution on $[a,b]$ represents the belief that the possible values of x are completely contained in the interval $[a,b]$ and $(d-c)/(b-a)$ is the probability that the value of x lies in the subinterval $[c,d]$ of $[a,b]$. However, if the information only supports the fact that $x \in [a,b]$, with no further reasons for different credibility of subsets of values within this set, then the assignment of a uniform distribution over $[a,b]$ does not appropriately characterize the information and knowledge available on the value of x.

Furthermore, the propagation of the uniform uncertainty of x onto functions of it, $y=f(x)$ (where f could be the model implemented in the computer code for the deterministic safety analysis), may lead to counterintuitive, non-uniform results if f is nonlinear. For example, if $y=x^2$ with x distributed uniformly on $[a,b]$ one would expect that nothing is known about the value of y except that it is contained in the interval $[a^2,b^2]$. On the contrary, this is not so: taking for instance $a=0$, $b=1$, indeed $y \in [0,1]$ but with non-uniform probability (for example, the probability that $y \leq 0.16$ is 0.4) [12].

As a result of the potential limitations associated to a probabilistic representation of epistemic uncertainty under limited quantitative information, a number of alternative representation frameworks have been proposed, e.g. fuzzy set theory [16-17], evidence theory [18], possibility theory [19] and interval analysis [20]. Evidence and possibility theories, in particular, may be the most attractive ones for risk assessment, because of their representation power and relative mathematical simplicity. They are similar to probability theory in that they are based on set functions but differ in that they make use of dual set functions.

Contrary to probability theory which assigns the probability mass to individual elementary events, the theory of evidence makes basic probability assignments $m(A)$ on sets A (the focal sets) of the power set $P(X)$ of the event space X, i.e. on sets of outcomes rather than on single elementary events. This allows the naturally encoding of evidence in favor of the different events which may occur.

Also, probability theory imposes more restrictive conditions on the specification of the likelihood of events as a result of the requirement that the probabilities of the occurrence and nonoccurrence of an event must sum to one.

As a result, while in probability theory, a single probability distribution function is introduced to define the probabilities of any event or proposition, represented as a subset of the sample space, in evidence and possibility theory there are two measures of likelihood, belief/plausibility and possibility/necessity, respectively. For example, the evidence theory framework allows for the belief about events and propositions to be represented as intervals, bounded by two values, belief and plausibility. The belief in a proposition is quantified as the sum of the probability masses assigned to all sets enclosed by it, i.e. the sum of the masses of all subsets of the proposition: hence, it is a lower bound representing the amount of belief that directly supports a given proposition at least in part. Plausibility is the sum of the probability masses assigned to all sets whose intersection with the proposition is not empty: hence, it is an upper bound on the possibility that the proposition could be verified, i.e. it measures the fact that the proposition could possibly be true "up to that value" because there is only so much evidence that contradicts it.

Both evidence and possibility theories allow epistemic uncertainty (imprecision) and aleatory uncertainty (variability) to be treated separately within a single framework. Indeed, the corresponding dual fuzzy measures provide mathematical tools to process information which is at the same time of random and imprecise nature [21-22].

In synthesis, while random variability can be adequately represented by probability distribution functions, imprecision or partial ignorance may be properly described in terms of belief functions and possibility distributions representing families of probability distributions [23]. Actually, the combination of the evidence or possibility and probability theories may prove powerful in providing an integrated framework of representation and analysis of uncertainties of both the aleatory and epistemic type [22, 24].

Regardless of which framework is adopted for handling epistemic uncertainty (the issue of which one is best suited for the different sources of uncertainty is still somewhat controversial and subject of further studies), the final objective is to produce insights in the analysis outcomes which can be meaningfully used by the decision makers. This entails that a number of topics be successfully addressed [12]:

- How to collect the information (e.g. in the form of expert judgment) and input it into the proper mathematical format.
- How to aggregate information from multiple, diverse sources into a single representation of uncertainty.
- How to propagate the uncertainty through the model so as to obtain the proper representation of the uncertainty in the output of the analysis.
- How to present and interpret the uncertainty results in a manner that is understandable and useful to decision makers.
- How to perform sensitivity analyses to provide insights with respect to which input uncertainties dominate the output uncertainties, so as to guide resources towards an effective uncertainty reduction.

3. DEMPSTER-SHAFER THEORY OF EVIDENCE

The Dempster-Shafer theory of evidence, also known as the theory of belief functions, is a generalization of the Bayesian theory of subjective probability in that it does not require probabilities for each proposition or event of interest but bases the belief in the truth of a proposition or occurrence of an event on the probabilities of other propositions or events related to it.

As such, it provides an alternative to the traditional manner in which probability theory is used to represent uncertainty by allowing less restrictive statements about likelihood than in the case of a probabilistic characterization of uncertainty. This relaxation is obtained by means of the specification of two degrees of likelihood, a *belief* and a *plausibility*, for each subset of the universal set under consideration.

The theory is based on two fundamental ideas: 1) the idea of obtaining degrees of belief for one question from subjective probabilities for related questions; 2) Dempster's rule for combining the degrees of belief when they are based on independent items of evidence. Before delving into the mathematical formulation, a simple illustrative example is discussed on an intuitive basis.

To illustrate the first idea of obtaining degrees of belief for one question from subjective probabilities for related questions, suppose that a diagnostic model is available to indicate with reliability (i.e. probability of providing the correct result) of 0.9 when a given system is failed. Considering a case in which the model does indeed indicate that the system is failed, this fact justifies a 0.9 degree of belief on such event (which is different from the related event of model correctness for which the probability value of 0.9 is available) but only a 0 degree of belief (not a 0.1) on the event that the system is not failed. This latter belief does not mean that it is certain that the system has failed, as a zero probability would: it merely means that the model indication provides no evidence to support the fact that the system is not failed. The pair of values {0.9, 0} constitutes a belief function on the propositions 'the system is failed' and 'the system is not failed'.

To illustrate Dempster rule for combining degrees of belief, suppose that there is available another model also capable of indicating system failure with reliability of 0.9 and also confirming the indication of system failure in this case. The probability that both models are providing the correct result is 0.81, that neither are correct is 0.01 and that at least one is correct is 0.99. Since both models are agreeing in identifying the state of the system as faulty, believing that the system failure event has occurred is equivalent to believing that at least one of them is correct: this leads to assigning a degree of belief of 0.99 to the system failure event.

On the contrary, if the two models contradict each other (the first model indicating a faulty state and the other a success state) they cannot both be correct. A priori of the system state indication, the probabilities that only the first model is correct, that only the second model is correct and that neither one is correct are 0.09, 0.09 and 0.01, respectively. A posteriori of the contradictory indication of system failure and success by the two models respectively, these probabilities become 9/19, 9/19 and 1/19, respectively. Hence, there is a 9/19 degree of belief associated to the event that the system has failed, deriving from the related reliability of the first model and an equal 9/19 degree of belief associated to the dual event of system success, deriving from the related reliability of the second model.

From the above simple example, one can appreciate how the degrees of belief for one question (has the system failed?) are obtained from probabilities related to another question (is the diagnostic model reliable?).

Dempster rule is based on the assumption that the questions for which probabilities are available are independent with respect to our subjective probability judgments; however, this independence is only a priori and readily disappears when conflict is discerned between the different items of evidence. This requirement of a priori independence entails framing the uncertainties affecting the problem in a way to work with independent items of evidence. Suppose for example that both models are identifying system failure based on the signals provided by a same sensor placed on the system: the two models might both be mistaken by a sensor reading error and because of this common uncertainty the two degrees of belief related to the event of system failure cannot be combined by Dempster rule. On the other hand, one may identify three independent pieces of evidence by introducing the evidence related to the sensor reading error and the associated probability. By so doing, the three pieces of evidence can be properly combined by Dempster rule.

One of the computational advantages of the Dempster-Shafer framework is that priors and conditionals need not be specified, unlike in Bayesian methods.

3.1 Mathematical Formulation

For the formal introduction of the Dempster-Shafer theory of evidence, let us consider the representation of the epistemic uncertainty in the attribution of an element x to a particular member A of a countable set. For example, suppose that x is a parameter whose values may vary in a given range X also called *Universe of Discourse* (UOD): then, the epistemic uncertainty associated to the attribution of x can be represented by assigning to each crisp set in X a value which represents the degree of evidence that x belongs to such set. This value is a *fuzzy measure* of the uncertainty in the assignment of x to a crisp set, which in itself is not uncertain.

At this point, it seems important to underline that the theory of fuzzy measures is different from the theory of fuzzy sets. The latter deals with the uncertainty associated with vague, linguistic statements represented by overlapping fuzzy sets, with no sharp boundaries; as a result of the vagueness in the available information, a given $x \in X$ may simultaneously belong to several sets with different degrees of membership.

Thus, the difference between a fuzzy measure and a fuzzy set is clear: the former represents the uncertainty in the assignment of an element to a given crisp set, due to lack of knowledge or information deficiency, whereas the latter represents the uncertainty in the definition of the boundaries of a set, due to a lack of sharp boundaries deriving from vague information [17].

For the formal definition of fuzzy measures, let us consider a finite UOD and an element $x \in X$ which is not fully characterized, i.e. it might belong to more than one crisp set in X. Let $P(X)$ denote the so called *power set of* X, i.e. the set of all subsets of X. For a given set $A \subseteq P(X)$, the uncertainty in the assignment of x to A can be quantitatively represented by the value of a function $g(A)$ which maps to $[0,1]$ the available evidence regarding the membership of x in A. This function is termed fuzzy measure and satisfies the *minitivity* and *maxitivity* constraints with respect to the conjunction and disjunction of two events A and B:

$$g(A \cap B) \leq \min[g(A), g(B)] \tag{1}$$

$$g(A \cup B) \geq \max[g(A), g(B)] \tag{2}$$

There are two forms of fuzzy measure functions, namely the *belief measure*, *Bel*(A), associated to preconceived notions, and the *plausibility measure Pl*(A), associated with plausible information.

The belief measure represents the *degree of belief*, based on the available evidence, that a given element of X belongs to A as well as to any of the subsets of A; it is the degree of belief in set A, based on the available evidence. In this sense, the different subsets of A may be viewed as the answers to a particular question, some of which are correct but it is not known which ones with full certainty.

A fundamental property of the belief function is that:

$$Bel(A) + Bel(\bar{A}) \leq 1 \tag{3}$$

Thus, the specification of the belief function is capable of incorporating a lack of confidence in the occurrence of the event defined by subset A, quantitatively manifested in the sum of the beliefs of the occurrence (*Bel*(A)) and non occurrence (*Bel*($\bar{A}$)) being less than one.

The difference 1-(*Bel*(A)+*Bel*($\bar{A}$)) is called *ignorance*. When the ignorance is 0, the available evidence justifies a probabilistic description of the uncertainty (see Section 3.3 below).

The plausibility measure can be interpreted as the total evidence that a particular element of X belongs not only to A or any of its subsets, as for *Bel*(A), but also to any set which overlaps with A.

A fundamental property of the plausibility function is that:

$$Pl(A) + Pl(\bar{A}) \geq 1 \tag{4}$$

Thus, the specification of the plausibility function is capable of incorporating a recognition of alternatives in the occurrence of the event defined by subset A, quantitatively manifested in the sum of the plausibilities of the occurrence (*Pl*(A)) and non occurrence (*Pl*($\bar{A}$)) being greater than one.

The links with the belief measure are:

$$Pl(A) = 1 - Bel(\bar{A}) \tag{5}$$

$$Bel(A) = 1 - Pl(\bar{A}) \tag{6}$$

from which,

$$Bel(A) \leq Pl(A) \tag{7}$$

The representation of uncertainty based on the above two fuzzy measures falls under the framework of *evidence theory* [18]. While in probability theory a single probability distribution function is introduced to define the probabilities of any event represented as a subset of the sample space, in evidence theory there are two measures of the likelihood, belief and plausibility. Also, in contrast to the inequalities (3) and (4), probability theory imposes more restrictive conditions on the specification of likelihood by requiring that the probabilities of the occurrence and nonoccurrence of an event must sum to one (see Eq. (19) below).

Being a generalization of the Bayesian theory of subjective probability, evidence theory allows epistemic uncertainty (imprecision) and aleatory uncertainty (variability) to be treated separately within a single framework. Indeed, the belief and plausibility functions provide mathematical tools to process information which is at the same time of random and imprecise nature.

3.2 Basic Probability Assignment

The belief and plausibility functions are defined from a mass distribution $m(A)$ on the sets A of the power set $P(X)$ of the UOD X, called *basic probability assignment (bpa)*, which expresses the degree of belief that a specific element x belongs to the set A only, and not to any subset of A. In other words, the mass $m(A)$ of a given member A of the power set expresses the proportion of all relevant and available evidence that supports the claim that the actual value of the parameter belongs to A but no particular subset of it.

The bpa satisfies the following requirements:

$$m : P(X) \rightarrow [0,1], \quad m(0) = 0; \ \sum_{A \in P(X)} m(A) = 1 \tag{8}$$

Suppose for example that a system has five independent states, one of which is the unknown true state. There are 2^5 possible subsets in the power set which the available evidence may support with respect to the state of the system; each subset can be represented by a binary array whose 5 elements indicate whether a particular state is occurring (1) or not (0). The empty subset (0,0,0,0,0) represents a contradiction which is never true as the system must be in a given state at all times; the 'every-possibility' or 'unknown' state (1,1,1,1,1) represents the situation in which the system may be in any state, in the sense that the available evidence does not allow to exclude anyone.

Note that from the definition (8), it is not required that $m(X)=1$, nor that $m(A) \leq m(B)$ when $A \subseteq B$, nor that there be any relationship between $m(A)$ and $m(\bar{A})$. Hence, the bpa is not a fuzzy measure, nor a probability distribution.

Further, note that contrary to probability theory which assigns the probability mass to individual values of x, the theory of evidence makes basic probability assignments $m(A)$ on sets A of the power set $P(X)$ of the UOD X, i.e. on sets of possibilities rather than single events, thus naturally encoding the evidence in favor of the different possibilities.

As mentioned above, for each set A of the power set $P(X)$, the bpa $m(A)$ expresses the proportion to which all available and relevant evidence supports the claim that a particular element x of X, whose characterization is incomplete, belongs to set A. The value of $m(A)$ pertains solely to set A and does not imply any additional claim regarding subsets of A; if there is additional evidence supporting the claim that the element x belongs to a subset of A, say $B \subseteq A$, it must be expressed by another probability assignment on B, i.e. $m(B)$.

Every set $A_i \in P(X)$ for which $m(A_i)>0$ is called a *focal element of m*: as the name suggests, focal elements are subsets of X which the available evidence allows to support to given degrees. When X is finite, the bpa m can be fully characterized by a list of its focal elements A_i with the corresponding values $m(A_i)$, which together quantify the *body of evidence* $\{A_i, m(A_i)\}$.

Total ignorance, then, amounts to the following assignment:

$$m(X) = 1; \quad m(A_i) = 0, \forall A_i \neq X \tag{9}$$

The bpa defines the belief and plausibility measures as follows,

$$Bel(A) = \sum_{B \subseteq A} m(B) \tag{10}$$

$$Pl(A) = \sum_{B \cap A \neq 0} m(B) \tag{11}$$

Thus, the belief for a set A is the sum of all the masses of subsets of A whereas the plausibility is the sum of all the masses of the sets B which intersect with A. Hence, the evidence theory framework allows for the belief about propositions or events to be represented as intervals, bounded by two values, belief and plausibility. The belief in a proposition is quantified as the sum of the masses of all sets enclosed by it, i.e. the sum of the masses of all subsets of the proposition. Hence, it represents the amount of belief that directly supports a given proposition at least in part, forming a lower bound. Plausibility is the sum of the masses of all sets whose intersection with the proposition is not empty. Hence, it is an upper bound on the possibility that the proposition could be verified, i.e. it measures the fact that the proposition could possibly be true "up to that value" because there is only so much evidence that contradicts it.

In the case of total ignorance,

$$Bel(X) = 1; \quad Bel(A_i) = 0, \forall A_i \neq X \tag{12}$$

$$Pl(X) = 1; \quad Pl(A_i) = 1, \forall A_i \neq 0 \tag{13}$$

In synthesis:

- $m(A)$ is the degree of evidence of membership in set A only; it is the amount of likelihood that is associated with A but without any specification of how this likelihood might be apportioned over A: this likelihood might be associated with any subset of A.

- $Bel(A)$ gathers the imprecise evidence that asserts A; it is the total evidence of membership in set A and all its subsets, which is quantified according to (10) as the minimal amount of probability that *must* be assigned to A by summing the pertinent probability masses of the single values in the focal sets: this amount of likelihood cannot move out of A because the summation in (10) involves only subsets B of A;
- $Pl(A)$ gathers the imprecise evidence that does not contradict A; it is the total evidence of membership in set A, including all its subsets and all other sets which intersect with A, and is quantified according to (11) as the maximal amount of probability that *could* be assigned to A by summing the pertinent probability masses of the single values in the focal sets: this amount of likelihood could move into A from another intersecting set, because the summation in (11) involves all sets B which intersect with A.

Then, an expert *believes* that the evidence supporting set A is at least $Bel(A)$ and *possibly as high as* $Pl(A)$.

With reference to the previous example of a diagnostic model indicating with reliability 0.9 that the system is failed, Table 1 reports the values of mass, belief and plausibility for the 2^2 possible propositions in the power set. Note that the belief for both the 'success' and 'failed' propositions matches their corresponding mass assignments, because these propositions have no subsets. Further, the 'unknown' proposition (either 'success' or 'failed') has always full belief and plausibility, by definition. The interval (belief, plausibility) represents the uncertainty on the probability of each proposition, based on the available evidence.

3.3 Relation to Probability Measures

Let us consider a bpa only on individual values (singletons) $x \in X$ but not on any other subset A of the power set $P(X)$, i.e. $m(x)=Bel(x), x \in X, m(A)=0, \ \forall A \in X$. Then, $m(x)$ is a probability measure, commonly denoted as $p(x)$, which maps the evidence on singletons to the unit interval [0,1].

It is then clear that the key distinction between a probability measure and either a belief or probability measure is that in the former all evidence is focused on singletons x only, whereas in belief and plausibility measures the evidence is focused on (focal) subsets A of the power set $P(X)$.

Obviously, from the probability measure $P(x)$ defined on all singletons $x \in X$ one can compute the probability measure $P(A)$ of any set A, which is simply a collection of singletons:

$$p(A) = \sum_{x \in A} p(x), \qquad \forall A \in P(X) \tag{14}$$

Notice that in this case in which the basic probability assignment focuses only on singletons $x \in X$, the belief, plausibility and probability of a set A are all equal:

$$Bel(A) = Pl(A) = p(A) = \sum_{x \in A} p(x) = \sum_{x \in A} m(x) \qquad \forall A \in P(X) \tag{15}$$

Thus, belief and plausibility measures overlap when all the evidence is focused only on singletons $x \in X$ and they both become probability measures.

Also, considering for simplicity only two focal sets A and B, a probability measure arises if:

$$Bel(A \cup B) = Bel(A) + Bel(B) \qquad A \cap B = 0 \tag{16}$$

$$Pl(A \cup B) = Pl(A) + Pl(B) \qquad A \cap B = 0 \tag{17}$$

On the contrary, when evidence does not reside exclusively on the singletons $x \in X$, it can be shown that

$$Bel(A) \leq p(A) \leq Pl(A) \tag{18}$$

Thus, the dual measures of belief and plausibility form intervals $[Bel(A), Pl(A)] \ \forall A \in P(X)$ which can be viewed as imprecise estimates of probabilities derived from the coarse evidence expressed by the basic probability assignment.

Table 1. Mass, Belief and Plausibility for the Success or Failed State of a System, Based on the Indication of a Fault by a Diagnostic Model with 0.9 Reliability

Proposition	Mass	Belief	Plausibility
Empty (neither success nor failed)	0	0	0
Success	0	0	0.1
Failed	0.9	0.9	1
Unknown (success or failed)	0.1	1	1

Finally, from (3), (4) and (15) it follows that

$$p(A)+p(\bar{A})=1 \tag{19}$$

which imposes a more stringent condition on the probability measure than (3) and (4) do on the belief and plausibility measures, respectively.

3.4 Aggregation of Multiple Sources of Evidence

In Dempster-Shafer Theory, evidence may be combined in different ways which range from conjunction (AND, based on the intersection of events or sets) to disjunction (OR, based on the union of events or sets) operators. If all sources are reliable, their conjunction pooling (A AND B AND C…) is appropriate; on the contrary, if there is one reliable source among many, the disjunctive pooling (A OR B OR C…) is justified; in practice, many combination operations lie between these two extremes in a *tradeoff* pooling effort.

The Dempster rule of combination is purely a conjunctive operation (AND) which combines multiple evidence through their basic probability assignments. It is a generalization of Bayes rule which emphasizes agreement among sources while ignoring all conflict through the introduction of a normalization factor.

Let us consider the common situation in which imprecise evidence is available from more than one source. For simplicity, let us consider two experts whose evidence is expressed in terms of two sets of bpa's, $m_1(A)$, $m_2(A)$ on the focal sets A of the power set $P(X)$ of X. The bpa functions on the frame of discernment are based on independent arguments and bodies of evidence, whose combination results in a belief function based on conjunctive pooled evidence [18]. Aggregation of this evidence into a joint bpa $m_{12}(A)$ can be obtained by means of *Dempster rule* [25]:

$$m_{12}(A)=\frac{\sum\limits_{B\cap C=A} m_1(B)m_2(C)}{1-K} \qquad \forall A\neq 0$$
$$m_{12}(0)=0 \tag{20}$$

where the complementary normalization factor K is given by

$$K=\sum_{B\cap C\neq 0} m_1(B)m_2(C) \tag{21}$$

According to (20) and (21) above, the degree of evidence $m_1(B)$ regarding focal set $B\in P(X)$, from the first source and the degree of evidence $m_2(C)$ focused on focal set $C\in P(X)$, from the second source, are aggregated by taking their product $m_1(B)m_2(C)$ focused on the intersection focal set $B\cap C=A$. This way of combining evidence sources is analogous to the way in which in probability theory joint probability density functions (pdfs) are calculated from two independent marginal pdfs and is thus justified on the same grounds. However, some intersections $B\cap C$ of different focal elements B and C, from the first and second source, may result in the same set A so that one must sum their product contribution to obtain $m_{12}(A)$. Furthermore, some of the intersections may be the empty set, for which $m_{12}(0)=0$. Then, introducing K as the sum of products $m_1(B)m_2(C)$ of all focal elements B of m_1 and C of m_2 such that $B\cap C\neq 0$(15), a normalized joint basic assignment m_{12} (as required by (4)) is obtained by dividing by 1-K. As K is determined by the sum of products of the bpa's of all sets where the intersection is non-null (15), it represents the basic probability mass associated with conflict; it is a measure of the amount of conflict between the two mass sets and the normalization factor 1-K has the effect of completely ignoring conflict by attributing any mass associated with conflict to the null set [26]. Consequently, counterintuitive results are obtained in the face of significant conflict among the sources of evidence, which has raised serious criticism to the formula.

Suppose for example that an automatic diagnostic tool and a plant operator are asked to assess a fault condition of a machinery, on the basis of observed signals related to its health state. The automatic diagnostic tool evaluates that the machinery has a fault of type 1 with probability 0.99 and no fault at all with probability 0.01; the expert operator assesses that the machinery has a fault of type 2 with probability of 0.99 but recognizes the possibility of the machinery being healthy, with probability of 0.01. In this situation, the joint basic probability assignment $m(\textit{no fault})=1=Bel(\textit{no fault})$, thus completely supporting the diagnosis which both diagnosticians consider very unlikely.

As a further example, consider two experts who are asked their opinions regarding a system failure which may occur due to component A, B or C failing [27]. The expert beliefs are summarized in Table 2; their combinations are given in Table 2; the resulting joint bpa's are summarized in Table 3, together with the belief and plausibility values. The conflict is K=0.99·0.01+0.99·0.01+0.99·0.99 =0.9999; the joint assignment concentrates all the basic probability mass on component B, which corresponds to a belief value $Bel(B)$=1, in spite of the highly conflicting evidence.

Finally, there are a number of considerations that need to be addressed when combining evidence in the framework of Dempster-Shafer theory, in particular with respect to the significance and relevance of conflict. These regard the evidence itself (type, amount and accuracy), the sources of information (type, number, reliability, dependency and conflict) and the context of the application. As a result, the aggregation of evidence from multiple sources may be pursued in a variety of possible

Table 2. Basic Probability Assignments of Experts 1 and 2

Expert/Component	A	B	C
1	$m_1(A)$=0.99	$m_1(B)$=0.01	$m_1(C)$=0
2	$m_2(A)$=0	$m_2(B)$=0.01	$m_2(C)$=0.99

Table 3. Combination of the Basic Probability Assignments of Experts 1 and 2

Expert 1/ Expert 2	A	B	C
A	$m_1(A)m_2(A)$=0	$m_1(A)m_2(B)$=0.0099	$m_1(A)m_2(C)$=0.9801
B	$m_1(B)m_2(A)$=0	$m_1(B)m_2(B)$=0.0001	$m_1(B)m_2(C)$=0.0099
C	$m_1(C)m_2(A)$=0	$m_1(C)m_2(B)$=0	$m_1(C)m_2(C)$=0

Table 4. Joint Basic Probability Assignments and Belief and Plausibility Values

Component	m_{12}	*Bel*	*Pl*
A	$m_{12}(A)$=0	*Bel*(A)=0	*Pl*(A)=0
B	$m_{12}(B)=\frac{0.01\cdot 0.01}{1-0.99\cdot 0.01-0.99\cdot 0.01-0.99\cdot 0.99}=1$	*Bel*(B)=1	*Pl*(B)=1
C	$m_{12}(C)$=0	*Bel*(C)=0	*Pl*(A)=0

combination rules, most of which are modifications to the original Dempster rule sharing the common first step of marginal bpa's multiplication to find the corresponding joint bpa's and then differing on how these are combined and where the probability mass associated to conflict is best allocated to properly represent the degree of conflict among the evidential sources. Indeed, the most critical issue of combining evidence in Dempster-Shafer theory regards the characterization of conflict among the sources of information and this should guide the final selection of the combination rule. In general, under situations of minimal or irrelevant conflict and reliable sources of information, a Dempster combination may be justified as it normalizes out the conflict and allows for the comparative assessment of the masses associated to the various events. As the level of relevant conflict increases, conflict must be explicitly represented in the basic probability assignment of the universal set X. Furthermore, when choosing a combination rule, it is important to identify the requirements of the pooling situation as disjunctive, conjunctive or tradeoff.

From the operational perspective, it would be important to establish a formal procedure for guiding the selection of the appropriate combination operation. Partial insights in the behavior of the combination operators may be gained from their algebraic properties [26]. Indeed, while there is yet no accepted method of combining dependent pieces of information, desirable algebraic properties of the resulting combination rules are *commutativity* ($A \times B$=$B \times A$), *idempotence* ($A \times A$=A), *continuity* ($A \times B$≈$A' \times B$ *when* A'≈A), *associativity* ($A \times (B \times C)$=$(A \times B) \times C$) [28].

4. POSSIBILITY THEORY

Possibility theory offers an alternative way for representing uncertainty [19] [29]. Like evidence theory, it involves the specification of two measures of likelihood, *necessity* and *possibility*, for each subset of the universal set under consideration. On the other hand, differently from evidence theory, which is closely related to probability theory, possibility theory is closely tied to fuzzy set theory.

Possibility theory may be introduced axiomatically in terms of fuzzy measures, as an interpretation of fuzzy sets or as a special case of evidence theory for consonant (i.e., non conflicting) evidence. This latter view is here taken, for a more coherent flow of the material contained in the paper. The illustration which follows is mainly based on [17].

Let us consider a *consonant* body of evidence, that is evidence which is allocated to the various subsets of the power set $P(X)$ of the universal set X so as to not conflict. For such body of evidence one has:

$$Bel(A \cap B) = \min[Bel(A), Bel(B)] \qquad \forall A, B \in P(X) \tag{22}$$

$$Pl(A \cup B) = \max[Pl(A), Pl(B)] \tag{23}$$

Comparing these equations with (1) and (2) in Section 3, one can see that the evidence theory applied to consonant evidence is based on the extreme values of fuzzy measures with respect to intersection and union of sets. The corresponding belief and plausibility measures are referred to as *necessity* η and *possibility* π, respectively. Accordingly, Eqs. (22) and (23) are re-written as

$$\eta(A \cap B) = \min[\eta(A), \eta(B)] \tag{24}$$

$$\pi(A \cup B) = \max[\pi(A), \pi(B)] \tag{25}$$

For a consonant body of evidence, the dual relationships (5) and (6) are written for necessity and possibility as

$$\pi(A) = 1 - \eta(\overline{A}) \tag{26}$$

$$\eta(A) = 1 - \pi(\overline{A}) \tag{27}$$

In addition, possibility and necessity measures constrain each other in a strong way:

Given the dual relationship of the two measures, the

$$\eta(A) > 0 \Rightarrow \pi(A) = 1 \tag{28}$$

$$\pi(A) < 1 \Rightarrow \eta(A) = 0 \tag{29}$$

treatment that follows will focus only on the possibility measure π.

4.1 Possibility Distribution Function

The possibility measure on subsets A of the power set $P(X)$ is defined from a *possibility distribution function* $r(x)$ which maps the singleton elements $x \in X$ into the unit interval [17], i.e.

$$r : X \to [0,1] \qquad r(x) = \pi(x) \tag{30}$$

This distribution relates to the possibility measure $\pi(A)$ of subset $A \in P(X)$ through the relationship:

$$\pi(A) = \max_{x \in A} r(x) \tag{31}$$

In other words, every possibility measure $\pi(A)$, $A \in P(X)$, is uniquely represented by the associated possibility distribution function $r(x)$, $x \in X$.

It is interesting to note the peculiarity of the definition of the possibility measure $\pi(A)$ which derives from properties ($r(x)$) of the individual elements $x \in X$ whereas probability, plausibility and belief are defined in terms of subsets A.

The possibility distribution $r(x)$ can be arranged as an ordered sequence of values

$$\underline{r} = (\rho_1, \rho_2, \cdots, \rho_n) \tag{32}$$

where $\rho_i = r(x_i)$, $\rho_i \geq \rho_j$ for $i < j$ and n is the length of the ordered possibility distribution.

Alternatively, every possibility measure can also be characterized by the n-tuple of basic probability assignments $\mu_i = m(A_i)$, $i=1,2,\cdots,n$, on the consonant body of evidence formed by the nested sets A_i, $i=1,2,\cdots,n$,

$$\underline{m} = (\mu_1, \mu_2, \cdots, \mu_n) \tag{33}$$

$$\sum_{i=1}^{n} \mu_i = 1 \tag{34}$$

Considering the possibility value of the generic singleton $x_i \in X$, $i=1,2,\cdots,n$, one can write from (31) and (32):

$$\rho_i = r(x_i) = \pi(x_i) = Pl(x_i) \tag{35}$$

and from the definition (11) of the plausibility measure,

$$Pl(x_i) = \sum_{k=i}^{n} \mu_k = \sum_{k=i}^{n} m(A_k) = \rho_i \tag{36}$$

or in a recursive form,

$$\mu_i = m(A_i) = \rho_i - \rho_{i+1} \tag{37}$$

where $\rho_{n+1}=0$ by convention. This leads to a set of equations for the ordered values ρ_i of the possibility distribution (32) in terms of the plausibility measure (34),

$$\begin{array}{lllll} \rho_1 = & \mu_1 + & \mu_2 + \cdots + & \mu_n = & Pl(x_1) \\ \rho_2 = & & \mu_2 + \cdots + & \mu_n = & Pl(x_2) \\ \vdots & & \vdots & & \\ \rho_n = & & & \mu_n = & Pl(x_n) \end{array} \tag{38}$$

Note that the first value of any ordered possibility distribution is always $\rho_1=1$.

Table 5. Basic Probability Assignments

Focal Elements A_i	System states	Diagnostic System 1 m_1	Diagnostic System 2 m_2	Singletons
	0	0	0	
1	C	0	0.1	x_1
2	B	0.2	0.1	x_2
3	$B \cup C$	0.3	0	x_3
4	A	0	0.1	x_4
5	$A \cup C$	0	0	x_5
6	$A \cup B$	0	0.3	x_6
7	$A \cup B \cup C$	0.5	0.4	x_7

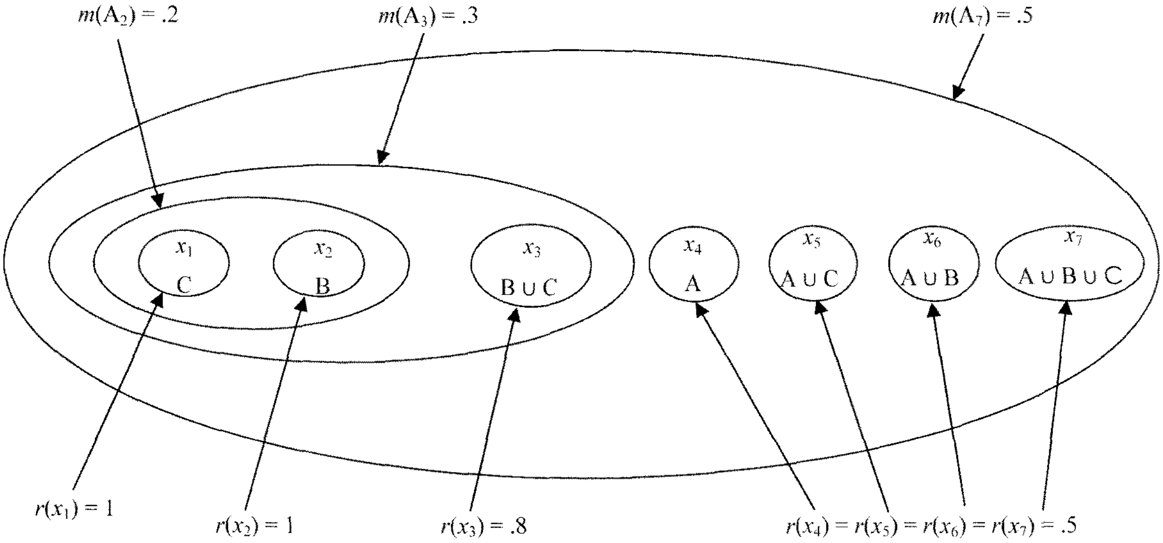

Fig 1. Nesting Diagram for the Evidence of Table 5 [17]

In general, the larger the possibility distribution the less specific the evidence and the more ignorance there is. The smallest possibility distribution describes the case where all the evidence is allocated onto one focal element, i.e.$\underline{r}=(1,0,\cdots,0)$ with corresponding basic probability assignment $\underline{m}=(1,0,\cdots,0)$. This situation of *perfect evidence* involves no uncertainty. Dually, the largest possible distribution is $\underline{r}=(1,1,\cdots,1)$, with corresponding basic probability assignment $\underline{m}=(0,0,\cdots,1)$ allocating all the evidence on the focal element comprising the entire universal set $X \equiv A_n = x_1 \cup x_2 \cup \cdots \cup x_n$. This represents the case where there is no specific knowledge about any particular focal element in the universal set, i.e. *total ignorance*.

In practice, one inspects the basic probability assignments $m(A_i)$ on the focal elements $A_i \in P(X)$ and verifies that they are consonant, i.e. not conflicting. A nested diagram can be drawn, with the nested sets embracing the appropriate subsets to form the focal elements. Then, Eqs. (36) or (38) allow retrieving the possibility distribution.

As an example [17], consider two diagnostic expert systems which are asked to identify the state of the system as healthy (A), degrading (B) or faulty (C), based on monitored data. Table 5 reports the basic probability assignments to the focal elements of the power set.

Based on the available data, expert system 1 assigns $m_1(B)$=0.2 to the degrading state, $m_1(B \cup C)$=0.3 to the degrading or faulty states and $m_1(A \cup B \cup C)$=0.5 to one of the three states. All the focal elements that have evidence are nested, i.e. $B \subset (B \cup C) \subset (A \cup B \cup C)$ and the basic distribution is

$$m_1 = (A_1, A_2, A_3, A_4, A_5, A_6, A_7) = (\mu_1, \mu_2, \mu_3, \mu_4, \mu_5, \mu_6, \mu_7) \\ = (0, 0.2, 0.3, 0, 0, 0, 0.5) \tag{39}$$

which from (35) produces the possibility distribution

$$r_1 = (1, 1, 0.8, 0.5, 0.5, 0.5, 0.5\ ) \tag{40}$$

The focal elements of expert system 1 can be represented in the nesting diagram of Fig 1, which indicates both the basic probability assignments to the nonzero elements A_2,A_3,A_7 and the possibility distributions for the various focal elements x_i, i=1,2,$\cdots$,7. On the contrary, for the expert system 2 the focal elements on m_2 are not nested since both sets C and B bear evidence but $C \not\subset B$.

4.2 Possibility Theory and Fuzzy Sets

Possibility theory can be formulated not only in terms of nested bodies of evidence, but also in terms of fuzzy sets [17]. Indeed, fuzzy sets are also based on families of nested sets, i.e. the *α-cuts*.

Consider a fuzzy set F on the universe of discourse X. The membership function $\mu_F(x)$, $x \in X$, represents the *degree of compatibility* of the value x with the linguistic concept expressed by F. On the other hand, with respect to the proposition X *is F* it is more meaningful to interpret $\mu_F(x)$ as the *degree of possibility* that X=F. According to this latter interpretation, the possibility $r_F(x)$ of X=x is numerically equal to the degree $\mu_F(x)$ with which x belongs to F:

$$r_F(x) = \mu_F(x) \qquad \forall x \in X \tag{41}$$

Then, the associated possibility measure π_F is defined for all $A \in P(X)$ by (31), viz.

$$\pi_F(A) = \max_{x \in A} r_F(x) \tag{42}$$

This measure expresses the uncertainty regarding the actual value of variable X under the incomplete information as given by the proposition X *is x*. For normal fuzzy sets, the associated necessity measure can be calculated for all $A \in P(X)$,

$$\eta_F(A) = 1 - \pi_F(\overline{A}) \qquad \forall A \in P(X) \tag{43}$$

For example, let X be a temperature variable taking only integer values. The available incomplete information about its value is given in terms of the proposition X *is around* $21°C$ as expressed by the fuzzy set F given in Fig 2a [17]. The incomplete information represented by fuzzy set F induces a possibility distribution function r_F that coincides with μ_F, according to (41) . The nested *α-cuts* of μ_F (Fig 2b) constitute the focal elements of the corresponding possibilistic body of evidence whose basic probability assignments, possibility and necessity measures are reported in Table 6.

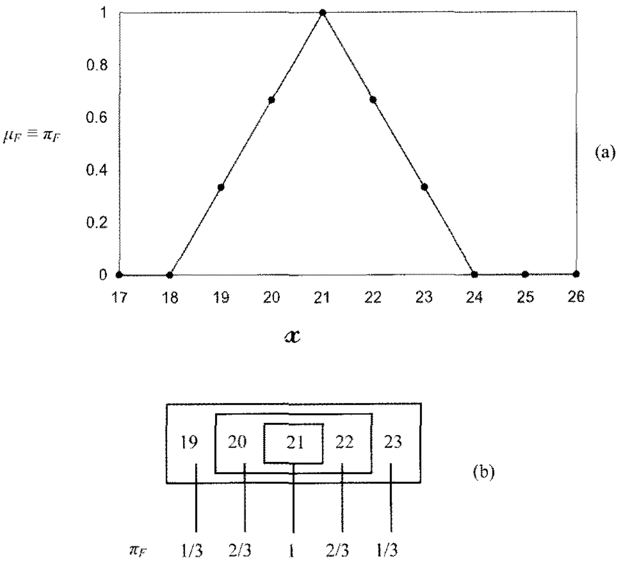

Fig 2. Fuzzy Set (a) and Corresponding Possibility Distribution over the Nested *α-cuts* (b) [17]

As mentioned earlier, formally possibility measures can be seen as equivalent to fuzzy sets. In this equivalence, the membership grade of an element x corresponds to the plausibility of the singleton consisting of that x. In other words, a consonant belief structure is equivalent to a fuzzy set F of X, where $\mu_F(x)$=$Pl(x)$.

A problem in equating consonant belief structures with fuzzy sets is that the combination of two consonant belief structures using Dempster rule (20)-(21) does not necessarily lead to a consonant result. Hence, since Dempster rule is essentially a conjunction operation, the intersection of two fuzzy sets interpreted as consonant belief structures may not result in a valid fuzzy set, i.e. a consonant structure.

Finally, while belief and plausibility measures overlap when all the evidence is only on singletons $x \in X$ and both become probability measures (Eq. 15), possibility, necessity and probability measures never overlap except for the special case of *perfect evidence* when all the body of evidence focuses on only one focal element, a singleton. The two distribution functions that represent possibilities and probabilities become equal in this case: one element of the universal set is assigned a value of unity whereas all other elements are assigned zero evidence.

4.3 Possibility Theory Versus Probability Theory

Possibility theory and probability theory are distinct theories and neither is subsumed under the other. Both

Table 6. Basic Probability Assignments, Possibility and Necessity Measures [17]

Set A_i	π	η	m
$A_1=\{21\}$	1	$\frac{1}{3}$	$\frac{1}{3}$
$A_2=\{20,21,22\}$	1	$\frac{2}{3}$	$\frac{1}{3}$
$A_3=\{19,20,21,22\}$	1	1	$\frac{1}{3}$

are special cases of Dempster-Shafer theory of evidence.

Table 7 summarises the main differences between the two theories [17]. Possibility theory is based on two dual measures, possibility and necessity, which are special versions of the belief and plausibility measures of Dempster-Shafer theory of evidence. Probability theory on the other hand, coincides with that sub-area of evidence theory in which belief measures and plausibility measures are equal. This difference results from a fundamental difference in the structure of the respective bodies of evidence: families of nested sets for the possibilistic ones and singletons for the probabilistic ones. As a consequence, also the normalization requirements are very different: for possibility distributions the largest values are required to be 1 whereas for probability distributions their values are required to sum to 1. These differences make each theory suitable for modelling certain types of uncertainty and less suitable for modelling other types.

A fundamental difference between the two theories lies in the way that total ignorance is represented: in possibility theory, as in evidence theory, this is achieved by setting $m(X)=1$, $m(A)=0$, $\forall A \neq X$ or equivalently $r(x)=1$, $\forall x \in X$; in probability theory, this is achieved by means of a uniform probability distribution over the universal set $p(x)=1/|X|$, $\forall x$. In particular, the probabilistic representation is justified by the fact that in probability theory every uncertain situation is represented by a single probability distribution. However, if no information is available to characterize the situation under study, then no distribution is supported by any evidence: total ignorance should thus be expressed in terms of the full set of possible probability distributions on X so that the probability of any value $x \in X$ is allowed to take any value in [0,1].

In any case, when information regarding some phenomenon is given in both probabilistic and possibilistic terms, the two descriptions should be in some sense consistent. In other words, the probability and possibility measures P and π defined on $P(X)$ should satisfy some consistency conditions.

The weakest, but most intuitive, consistency condition is

$$p(A) \le \pi(A) \qquad \forall A \in P(X) \tag{44}$$

This requires that an event that is probable to some degree must be possible at least to the same degree. The strongest consistency condition would require, on the other hand, that any event with nonzero probability must be fully possible, viz.

$$p(A) > 0 \Rightarrow \pi(A) = 1 \quad \forall A \in P(X) \tag{45}$$

In various applications, probability-possibility transformations are necessary, whose consistency needs to be assured. Several types of transformations exist, ranging from simple ratio scaling to more sophisticated operations. A degree of consistency between the probability and possibility measures may be defined as follows, in terms of the associated distributions:

$$c(p,r) = \sum_{x \in X} p(x) r(x) \tag{46}$$

5. COMBINING PROBABILITY AND POSSIBILITY IN UNCERTAINTY PROPAGATION

As highlighted in the opening Sections of the paper, the treatment of uncertainty is an issue of paramount importance for risk-informed applications. In particular with respect to the risk assessment component of risk-informed applications, the treatment of the epistemic uncertainty associated to the probability of occurrence of an event is fundamental. Traditionally, probabilistic distributions have been used to characterize such epistemic uncertainty, which is due to imprecise knowledge of the parameters in the risk models. On the other hand, in the preceding Sections it has been argued that in certain instances such uncertainty may be best accounted for by fuzzy or possibilistic distributions. This seems the case in

Table 7. Differences Between Possibility and Probability Theory [17]

Probability Theory	**Possibility Theory**
Based on a single measure, probability p	Based on two measures, possibility π and necessity η
Body of evidence consists of singletons	Body of evidence consists of a family of nested subsets
Unique representation of probability through a probability distribution function $p: X \rightarrow [0,1]$ via the formula $p(A)=\sum_{x\in A} p(x)$	Unique representation of possibility through a possibility distribution function $r: X \rightarrow [0,1]$ via the formula $\pi(A)=\max_{x\in A} r(x)$
Normalization: $\sum_{x\in X} p(x)=1$	Normalization: $\max_{x\in X} r(x)=1$
Additivity: $p(A\cup B)=p(A)+p(B)-p(A\cap B)$	Max/min rules: $\pi(A\cup B)=\max[\pi(A),\pi(B)]$ $\eta(A\cap B)=\min[\eta(A),\eta(B)]$
	$\eta(A)=1-\pi(\bar{A})$ $\pi(A)<1 \Rightarrow \eta(A)=0$ $\eta(A)>0 \Rightarrow \pi(A)=1$
$p(A)+p(\bar{A})=1$	$\pi(A)+\pi(\bar{A})\geq 1$ $\eta(A)+\eta(\bar{A})\leq 1$ $\max[\pi(A),\pi(\bar{A})]=1$ $\min[\eta(A),\eta(\bar{A})]=0$
Total ignorance: $p(x)=\frac{1}{\lvert X\rvert} \quad \forall x\in X$	Total ignorance: $r(x)=1 \quad \forall x\in X$
Conditional probabilities: $p_{X\mid Y}(x\mid y)=\frac{p_{XY}(x,y)}{p_Y(y)}$ $p_{Y\mid X}(y\mid x)=\frac{p_{XY}(x,y)}{p_X(x)}$	Conditional possibilities: $r_{X\mid Y}(x\mid y)=\begin{cases} r_X(x) & \textit{for } r_X(x)<r_Y(y) \\ [r_Y(y),1] & \textit{for } r_X(x)\geq r_Y(y) \end{cases}$ $r_{Y\mid X}(y\mid x)=\begin{cases} r_Y(y) & \textit{for } r_Y(y)<r_X(x) \\ [r_X(x),1] & \textit{for } r_Y(y)\geq r_X(x) \end{cases}$
Probabilistic non-interaction: $p_{XY}(x,y)=p_X(x)\,p_Y(y)$ (a) Probabilistic independence $p_{X\mid Y}(x\mid y)=p_X(x)$ $p_{Y\mid X}(y\mid x)=p_Y(y)$ (b)	Possibilistic non-interaction: $r(x,y)=\min[r_X(x), r_Y(y)]$ (a) Possibilistic independence $r_{X\mid Y}(x\mid y)=r_X(x)$ $r_{Y\mid X}(y\mid x)=r_Y(y)$ (b)
$(a) \Leftrightarrow (b)$	$(b) \Rightarrow (a)$ but not vice versa

particular for parameters for which the information available is scarce and of qualitative nature.

In practice, it is to be expected that a risk model contains some parameters affected by uncertainties which may be best represented by probability distributions and some other parameters which may be more properly described in terms of fuzzy or possibilistic distributions. In this Section, an hybrid method which jointly propagates probabilistic and possibilistic uncertainties is considered [22].

Let us consider a model whose output is a function $f(\cdot)$ of n input variables Y_j, $j=1,\cdots,n$; the uncertainty in the first k input variables (hereafter called 'probabilistic' variables) is characterized by probability distributions $p_{Y_j}(y)$ whereas the uncertainty in the last n-k input variables (hereafter called 'possibilistic' variables) is represented in terms of possibility distributions $\pi^{Y_j}(y)$ measuring the degree of possibility that the linguistic variables Y_j be equal to y. For the propagation of such mixed uncertainty information, the Monte Carlo technique [30] can be combined with the extension principle of fuzzy set theory [16] by means of the following two main steps [21]:

i. repeated Monte Carlo sampling of the probabilistic variables to process their uncertainty;

ii. fuzzy interval analysis to process the uncertainty connected with the possibilistic variables.

For the generic *i-th k-tuple* of random values, $i=1,2,\cdots,m$ sampled by Monte Carlo from the probabilistic distributions, a fuzzy set π_i^f estimate of $f(Y)$ is constructed by fuzzy interval analysis. After m repeated samplings of the probabilistic variables, the fuzzy set estimates π_i^f, $i=1,\cdots,m$, are combined to give an estimate of $f(Y)$ as a fuzzy random variable (or random possibility distribution) accordingly to the rules of evidence theory [18].

The operative steps of the procedure are:

1. sample the *i-th* realization $(y_1^i,\cdots,y_k^i)$ of the probabilistic variable vector $(y_1,\cdots,y_k)$
2. select a possibility value α and the corresponding cuts of the possibility distributions $(\pi^{Y_{k+1}},\cdots,\pi^{Y_n})$ as intervals of possible values of the possibilistic variables $(Y_{k+1},\cdots,Y_n)$
3. compute the smallest and largest values of $f(y_1^i,\cdots,y_k^i,Y_{k+1},\cdots,Y_n)$, denoted by $\underline{f}^i_\alpha$ and $\overline{f}^i_\alpha$ respectively, considering the fixed values $(y_1^i,\cdots,y_k^i)$ sampled for the random variables $(Y_1,\cdots,Y_k)$ and all values of the possibilistic variables $(Y_{k+1},\cdots,Y_n)$ in the *α-cuts* of their possibility distributions $(\pi^{Y_{k+1}},\cdots,\pi^{Y_n})$. Then, take the extreme values $\underline{f}^i_\alpha$ and $\overline{f}^i_\alpha$ found in 3. as the lower and upper limits of the *α-cut* of $f(y_1^i,\cdots,y_k^i,Y_{k+1},\cdots,Y_n)$
4. return to step 2 and repeat for another α-cut; after having repeated steps 2-3 for all the α-cuts of interest, the fuzzy random realization (fuzzy interval) π_i^f of $f(Y)$ is obtained as the collection of the values $\underline{f}^i_\alpha$ and $\overline{f}^i_\alpha$; in other words, π_i^f is defined by all its α-cut intervals $|\underline{f}^i_\alpha, \overline{f}^i_\alpha|$
5. return to step 1 to generate a new realization of the random variables.

The above procedure is repeated for $i=1,\cdots,m$; at the end of the procedure an ensemble of realizations of fuzzy intervals is obtained, i.e.$(\pi_1^f,\cdots,\pi_m^f)$. For each set A contained in the universe of discourse U_X of the output variable X, it is possible to obtain the possibility measure $\Pi_i^f(A)$ and the necessity measure $N_i^f(A)$ from the corresponding possibility distribution $\pi_i^f(u)$, by:

The m different realizations of possibility and necessity

$$\Pi_i^f(A)=\max_{u\in A}\{\pi_i^f(u)\} \quad \text{and}$$
$$N_i^f(A)=\inf_{u\notin A}\{1-\pi_i^f(u)\}=1-\Pi_i^f(\overline{A}) \qquad \forall A\subseteq U_X \tag{47}$$

can be combined to obtain the believe B*el*(*A*) and the plausibility $Pl(A)$ for any set A, respectively [21]:

$$Bel(A)=\sum_i p_i N_i^f(A) \qquad Pl(A)=\sum_i p_i \Pi_i^f(A) \tag{48}$$

where p_i is the probability of sampling the *i-th* realization $(y_1^i,\cdots,y_k^i)$ of the random variable vector $(Y_1,\cdots,Y_k)$. For each set A, this technique thus computes the probability-weighted average of the possibility measures associated with each output fuzzy interval.

The likelihood of the value $f(Y)$ passing a given threshold u can then be computed by considering the believe and the plausibility of the set $A=(-\infty,u]$; in this respect, $Bel(f(Y)\in(-\infty,u])$ and $Pl(f(Y)\in(-\infty,u])$ can be interpreted as bounding, average cumulative distributions $\underline{F}(u)=Bel(f(Y)\in(-\infty,u]),\ \overline{F}(u)=Pl(f(Y)\in(-\infty,u])$ [21].

Let the *core* and the *support* of a possibilistic distribution $\pi^f(u)$ be the crisp sets of all points of U_X such that $\pi^f(u)$ is equal to 1 and non zero, respectively. Considering a generic value u of $f(Y)$, it is $Pl(f(Y)\in(-\infty,u])=1$ if and only if $\Pi_i^f(f(Y)\in(-\infty,u])=1$, $\forall\, i=1,\cdots,m$, i.e. for $u>u^*=\max_i\{\inf(core(\pi_i^f))\}$. Similarly, $Pl(f(Y)\in(-\infty,u])=0$ if and only if $\Pi_i^f(f(Y)\in(-\infty,u])=0$, $\forall\, i=1,\cdots,m$, i.e. for $u\leq u_*=\min_i\{\inf(support(\pi_i^f))\}$.

Finally, one way to estimate the total uncertainty on $f(Y)$ is to provide a confidence interval at a given level of confidence, taking the lower and upper bounds from $Pl(f(Y)\in(-\infty,u])$ and $Bel(f(Y)\in(-\infty,u])$, respectively [21]. On the other hand, $Bel(f(Y)\in(-\infty,u])$ and $Pl(f(Y)\in(-\infty,u])$ cannot convey any information on the prediction that $f(Y)$ lies within a given interval $[u_1,u_2]$, since neither $Bel(f(Y)\in[u_1,u_2])$ nor $Pl(f(Y)\in[u_1,u_2])$ can be expressed in terms of $Bel(f(Y)\in(-\infty,u])$ and $Pl(f(Y)\in(-\infty,u])$, respectively.

5.1 Case Study

The approach for uncertainty propagation just illustrated has been applied [22] to the event tree analysis of an Anticipated Transient Without Scram (ATWS) event in a nuclear power plant in Taiwan [31]. Some results of this application are illustrated in the following.

The event tree in Fig 3 is considered, taken from Taiwan's nuclear power plant II operating PRA draft report [32]. The description of the headings of the tree are reported in Table A1 of the Appendix. According to the assumptions made [32], the probabilities of occurrence of

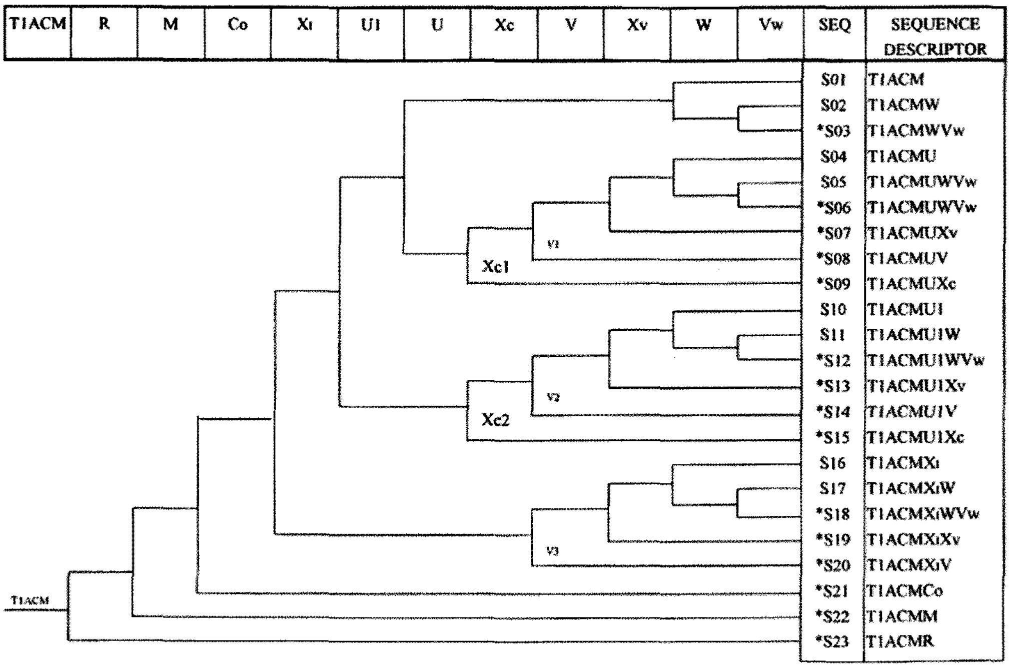

Fig 3. The Event Tree [31]; Upper Branch Corresponds to the Non-Occurrence of the Event, Lower Branch to the Occurrence, SEQ=Sequence Number, *=Severe Consequence Sequence

events X_C and V are conditioned by the occurrence of events U_I and X_I, whereas the probabilities of events X_v, W, V_W are considered as constants in the different sequences.

Two kinds of information are available with respect to the event occurrences. Adopting the same assumptions of [31], sufficient experimental data are available to build lognormal probability distributions $p_{vj}(v)$ representing the epistemic uncertainty in the event probabilities v_j, $j=1,\cdots,k$, for the $k=11$ hardware-failure-dominated (HFD) events. Table A2 in the Appendix reports the corresponding means and standard deviations. On the contrary, there are not enough data to build probability distributions for the human-error-dominated events: in this case, the knowledge of four experts has been elicited in the form of possibility distributions $\pi^{vj}(v), j=12,13,14,15$ (Fig A1 in the Appendix) [31].

The approach of joint uncertainty propagation described above has been applied to the computation of the probabilities of occurrence of the 23 accident sequences identified in the event tree of Fig 3. With respect to the mathematical formulation of the method, the function f_r, $r=1,\cdots,23$, used to compute the probability of occurrence of the r-th accident sequence, p_{Seq_r}, is the product of the probabilities v_j of occurrence/non occurrence of the single events along the sequence, i.e.

$$p_{Seq_r} = f_r(v_1,v_2,\ldots,v_{15}) = \prod_{j\ occurs\ in\ Seq_r} v_j \prod_{j\ does\ not\ occur\ in\ Seq_r} (1-v_j) \qquad r=1,\ldots,23 \tag{49}$$

From these sequence probabilities one can compute the probability of occurrence of severe consequences, p_{Sev}, by summing the probabilities of all the sequences that lead to severe consequences:

$$p_{Sev} = \sum_{r:\ Seq_r\ is\ Sev} p_{Seq_r} \tag{50}$$

Then, for all sets $A=[0,u), u\in R^+$, the possibility and the necessity measures, $\Pi_i^f([0,u))$ and $N_i^f([0,u))$, are obtained from the corresponding possibility distributions $\pi_i^f(u)$, according to Eq.(47).

Finally, the $m=1000$ possibility and necessity measures are combined to obtain the plausibility and necessity by (Eq. 48):

$$Bel([0,u)) = \sum_{i=1}^{m} \frac{1}{m} N_i^f([0,u)) \text{ and } Pl([0,u)) = \sum_{i=1}^{m} \frac{1}{m} \Pi_i^f([0,u)) \tag{51}$$

Fig 4 reports the believe and plausibility of the set $[0,u)$ obtained for the probabilities of occurrence of sequences 13, 15, 22 and of a severe consequence accident. The three sequences have been chosen because representative of distinct interesting cases of uncertainty propagation; on the other hand, the probability of a severe consequence accident is an important quantity for the evaluation of the risk.

In the top graph, notice that the $Bel([0,u))$ (lower curve) and the $Pl[0,u)$ (upper curve) of the probability of sequence

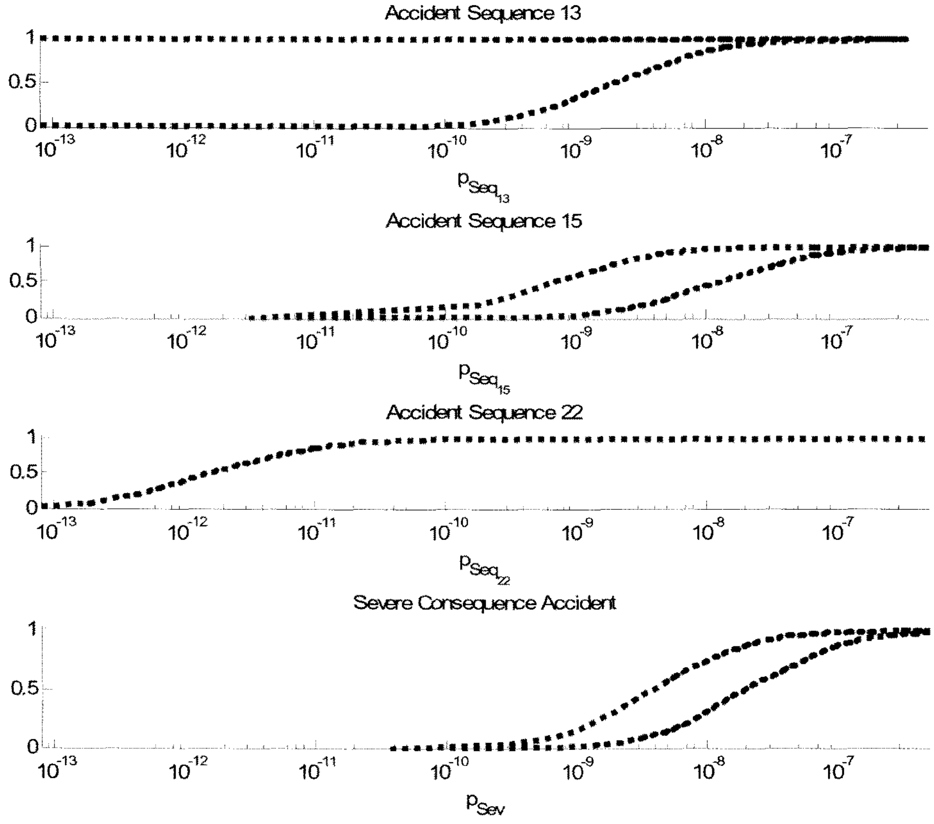

Fig 4. Believe and Plausibility of the Set [0,u) Resulting from Application of the Hybrid Approach

13 are quite far from one another indicating large imprecision in the estimation of the probability that $p_{13}<u$, i.e. of the cumulative distribution function $F(u)$. This is mainly due to the fact that Sequence 13 is characterized by the non occurrence of the human-error-dominated event Xc2 that is known only with very large imprecision (bottom left graph in Fig A1). For example, the value of *Pl*(0), that represents the plausibility of the impossibility of the occurrence of accident sequence 13, is equal to 1 while the *Bel*(0) that represents the necessity is equal to 0. The plausibility measure is 1 due to the fact that the possibility of having $v_{14}=1$ is 1, i.e. the expert believes that it is possible that event Xc2 always occurs; on the contrary, event Xc2 appears in Sequence 13 as not occurring, so that it is plausible that Sequence 13 never occurs ($Pl(p_{\mathrm{Seq}_{13}}=0)=1$).

The opposite occurs for the case of Sequence 22 characterized by the occurrence of only hardware-failure-dominated events. In this case, the input (probabilistic) variables v_1,v_2, of function f_{22} are represented by probabilistic distributions not affected by imprecision and thus *Bel*([0,*u*)) and *Pl*([0,*u*)) coincide and can be interpreted as the cumulative distribution function $F(u)$ (third graph from the top in Fig 4).

An intermediate situation between the cases of sequences 13 and 22 is represented by sequence 15 (second graph from the top of Fig 4). In this case the estimation of the probability of occurrence of the accident sequence, characterized by the presence of both human-error-dominated and hardware-failure-dominated events, is affected by both imprecision and variability represented by the gap between *Bel*([0,*u*)) and *Pl*([0,*u*)), and the slopes of the two curves, respectively.

6. CONCLUSIONS

Uncertainty is a key issue in all risk applications. For practical purposes, it is convenient to consider it as of two different types: i) aleatory, due to inherent randomness in the system behavior and ii) epistemic, due to imprecise knowledge and lack of information on the system. Such distinction plays a relevant role in the risk assessment framework applied to complex engineered systems such as the nuclear power plants.

In particular, in the current practice of risk-informed regulations and applications all uncertainties, epistemic or aleatory, are represented by means of probability distributions and their propagation is carried out by a two-loops Monte Carlo simulation where in the outer loop the values of the parameters (e.g. failure rates) affected by epistemic uncertainty are sampled and in the inner loop the aleatory variables (e.g. failure times) are sampled from the probability distributions conditioned at the values of the epistemic parameters sampled in the outer loop. However, resorting to a probabilistic representation of epistemic uncertainty may be difficult when sufficiently informative data is not available for statistical analysis, even if one adopts expert elicitation procedures within a subjective view of probability. Indeed, an expert may not have sufficiently refined knowledge or opinion to characterize the relevant epistemic uncertainty in terms of probability distributions. As a result of the potential limitations associated to a probabilistic representation of epistemic uncertainty under limited information, a number of alternative representation frameworks have been proposed, e.g. fuzzy set theory, evidence theory, possibility theory, probability bounds and interval analysis and imprecise probability.

In this work, the basic principles of the Dempster-Shafer theory of evidence have been recalled together with its specification into possibility theory. These theories offer alternative frameworks of representation which may add value to the treatment of uncertainty in risk-informed applications, particularly with respect to the epistemic uncertainty arising from incomplete knowledge of the parameters of the deterministic and probabilistic models used for the evaluation of risk.

An example is provided of the combined use of probabilistic and possibilistic representations of the uncertainties regarding the probability of occurrence of the events of an event tree. Events whose uncertain probabilities of occurrence can typically be described by probabilistic distributions are basic hardware failures, whereas for the probabilities of occurrence of human errors or of failures to protective or automation systems possibilistic distributions may be more appropriate. In general, an event tree may contain events of both kinds. The propagation of the epistemic uncertainty of these events can be carried out jointly as follows: Monte Carlo sampling of the random variables is repeatedly performed to process the epistemic uncertainty related to the events whose probabilities of occurrence are described by probabilistic distributions; then, fuzzy interval analysis is carried out at each sampling to process the epistemic uncertainty associated to the events whose probabilities of occurrence are described by possibilistic distributions. The application of the method results in the estimation of upper and lower cumulative distributions of the probabilities of occurrence of the accident sequences, while effectively distinguishing between the uncertainties due to events whose probability of occurrence is described by probabilistic or possibilistic distributions: the former are reflected by the slope of the believe and plausibility functions while the latter are pictured in the gap between the two functions.

As a final remark, it is important to underline that the acceptance in practice of uncertainty representation frameworks alternative to the probabilistic one is still very controversial. Although all the different frameworks proposed have the required axiomatic basis, the interpretation of the underlying concepts (in terms of metaphors, e.g. betting, and standards, e.g. drawing balls from an urn) and the associated quantitative measures, which are of key interest for practical applications, are simpler and more precisely defined for some than for others.

REFERENCES

[1] M. Modarres, *Advanced Nuclear Power Plant Regulation Using Risk-Informed and Performance-Based Methods*, Reliability Engineering and System Safety, 2008, doi:10.1016/j.ress.2008.02.019.

[2] IAEA, *Risk informed regulation of nuclear facilities: overview of the current status*, IAEA-TECDOC-1436, 2005.

[3] F.R. Farmer, *The Growth of Reactor Safety Criteria in the United Kingdom*, Anglo-Spanish Power Symposium, Madrid, 1964.

[4] Garrick, B.J. and Gekler, W.C., *Reliability Analysis of Nuclear Power Plant Protective Systems*, US Atomic Energy Commission, HN-190, 1967.

[5] WASH-1400, *Reactor Safety Study*, US Nuclear Regulatory Commission, 1975.

[6] U.S. Nuclear Regulatory Commission Regulatory Guide 1.174, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis*, USNRC, Regulatory Guide 1.1.74, Revision 1, November 2002.

[7] U.S. Nuclear Regulatory Commission Regulatory Guide 1.175, *An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Testing*, USNRC, August 1998.

[8] U.S. Nuclear Regulatory Commission Regulatory Guide 1.176, *An Approach for Plant-Specific, Risk-Informed Decisionmaking: Graded Quality Assurance*, USNRC, August 1998.

[9] U.S. Nuclear Regulatory Commission Regulatory Guide 1.177, *An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications*, USNRC, August 1998.

[10] A.C. Kadak and T. Matsuo, *The Nuclear Industry's Transition to Risk-Informed Regulation and Operation in the United States*, Reliability Engineering and System Safety, Vol. 92, 2007, pp. 609-618.

[11] G.E. Apostolakis, *The Concept of Probability in Safety Assessments of Technological Systems*, Science, 1990, pp. 1359-1364.

[12] J.C. Helton, *Alternative Representations of Epistemic Uncertainty*, Special Issue of Reliability Engineering and System Safety, Vol. 85, 2004.

[13] K.-Y Cai., *System Failure Engineering and Fuzzy Methodology. An Introductory Overview*, Fuzzy Sets and Systems 83, 1996, pp. 113-133.

[14] Da Ruan, J. Kacprzyk and M. Fedrizzi, *Soft Computing for Risk Evaluation and Management*, Physica-Verlag, 2001.

[15] *Soft Methods in Safety and Reliability, Special Sessions I-III*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1.

[16] L.A. Zadeh, *Fuzzy Sets*, Information and Control, Vol. 8, 1965, pp. 338-353.

[17] G.J. Klir and B. Yuan, *Fuzzy Sets and Fuzzy Logic: Theory and Applications*, Upper Saddle River, NJ, Prentice-Hall, 1995.

[18] G. Shafer, *A Mathematical Theory of Evidence*, University Press, Princeton, 1976.

[19] D. Dubois and H. Prade, *Possibility Theory: An Approach to Computerized Processing of Uncertainty*, New York, Plenum Press, 1988.

[20] R.E. Moore, *Methods and Applications of Interval Analysis*, Philapdelphia, PA: SIAM, 1979.

[21] C. Baudrit, D. Dubois and D. Guyonnet, *Joint Propagation of Probabilistic and Possibilistic Information in Risk Assessment*, IEEE Transactions on Fuzzy Systems, Vol. 14, 2006, pp. 593-608.

[22] P. Baraldi and E. Zio, *A Combined Monte Carlo and Possibilistic Approach to Uncertainty Propagation in Event Tree Analysis*, 2008.

[23] D. Dubois, *Possibility Theory and Statistical Reasoning*, Computational Statistics and Data Analysis, Vol. 51, 2006, pp. 47-69.

[24] C. Baudrit and D. Dubois, *Practical Representations of Incomplete Probabilistic Knowledge*, Computational Statistics and Data Analysis, Vol. 51, 2006, pp. 86-108.

[25] A.P. Dempster, *Upper and Lower Probabilities Induced by a Multivalued Mapping*, Ann. Mat. Stat., Vol. 38, 1967, pp. 325-339.

[26] R. Yager, *On the Dempster-Shafer Framework and New Combination Rules*, Information Sciences, Vol. 16, pp. 37-41.

[27] K. Sentz and S. Ferson, *Combination of Evidence in Dempster-Shafer Theory*, SAND 2002-0835, Sandia National Laboratories, USA.

[28] S. Ferson and V. Kreinovich, Representation, Propagation and Aggregation of Uncertainty, SAND Report.

[29] G. de Cooman, *Possibility Theory Part I : Measure- and Integral-Theoretic Groundwork; Part II: Conditional Possibility; Part III: Possibilistic Independence*, Int. J. Gen. Syst., 1997, Vol. 25 (4), pp. 291-371.

[30] M. H. Kalos, P. A. Whitlock, *Monte Carlo methods. Volume I: Basics*, Wiley, 1986.

[31] D. Huang, T. Chen, M. J. Wang, *A fuzzy set approach for event tree analysis*, Fuzzy Sets ans Systems 118, pp 153-165, 2001.

[32] Nuclear Power Plant 2 Operating Living PRA Report (Draft). Nuclear Energy Research Center, Tao Yuan, Taiwan, 1995.

APPENDIX

Table A1. Event Tree Headings (Top Events) [31]; v = Probability of Occurrence, HFD = Hardware-Failure-Dominated, HED = Human-Error-Dominated

Event	Acronym	Type	v	Description
main condenser isolation ATWS	T1ACM	HFD	v_1	*This event will happen when the reactor is isolated and the automatic scram system fails. It is also assumed that mechanical failures cannot be repaired within the allowable time.*
recirculation pump trip	R	HFD	v_2	*If the plant fails to scram, an automatic recirculation pump system is required to limit power generation immediately. A failure of the automatic recirculation pump system will result in event R.*
safety/relief valves (S/RVs) open	M	HFD	v_3	*At the time the reactor is isolated, at least 13 of 16 S/RVs must open to prevent overpressurization of the reactor vessel. If insufficient S/RVs open, then event M will happen.*

Boron injection	C_0	HFD	v_4	*When an ATWS event happens, the power of the core is very high. If the power cannot be slowed down to the state of shutdown, and the vapor produced by the reactor continues to inject into the suppression pool, then the temperature will increase to fail the high-pressure system. This will increase the possibility of core meltdown. As a result, automatic redundant reactivity control system (RRCS) is supposed to inject liquid Boron into the vessel to shut down the reactor safely. If automatic RRCS fails, and operators fail to inject liquid Boron by using standby liquid control system (SLCS), it will result in event C_0. It is assumed that operators cannot manually inject liquid Boron within the allowable time.*
ADS inhibit	X_I	HED	v_{12}	*Automatic depressurization system (ADS) is designed to decrease the pressure of the reactor in order to start the low-pressure system. The low-pressure system will inject water into the reactor vessel to protect the fuel. When an ATWS event happens, the reactor power is controlled by the level of water in core. Since high-level water will cause high power, the operator should inhibit all ADS valves manually. If the operator fails to do so, event X_I will occur.*
early high-pressure makeup	U1	HFD	v_5	*Following the stop of feedwater supply, the high-pressure makeup system is supposed to work automatically when automatic actuation alarm appears as soon as the water level is lowering till level 2. The water level is expected to reach the top of the fuel. Thus, if the high-pressure system fails to work automatically, it will lead to event U1.*
long-term high-pressure makeup	U	HFD	v_6	*The success criterion of avoidance of this event is that the high-pressure system can maintain the water level in the vessel 24 h after the start. If the system fails and causes event U, then using the low-pressure system to maintain the water level is needed.*
manual reactor depressurization	X_C (X_{C1},X_{C2})	HED	v_{13},v_{14}	*If the pressure in the reactor vessel is too high to set up the low-pressure system, the operator should depressurize the vessel manually in time to avoid core melt-down. Due to the different conditional probabilities of occurrence of this event in different accidental sequences, X_c is called X_{c1} in sequences 4-9 characterized by the non-occurrence of event U1 and X_{c2} in sequences 10-15 characterized by the occurrence of event U1.*

reactor inventory makeup at low pressure	V (V_1,V_2,V_3)	HFD	v_7,v_8,v_9	*If the low-pressure system fails as well as the high-pressure system, then event V will occur and the water level in the vessel will be so low as to probably cause core melt-down. Due to the different conditional probabilities of occurrence of this event in different accidental sequences, V is called V1 in sequences 4-7, V_2 in sequences 10-14 and V_3 in sequences 16-20.*
vessel overfill prevention	X_V	HED	v_{15}	*When the pressure in the vessel is decreased till the level low enough for the low-pressure system to inject water, huge amount of water will come into the core. The operator should pay attention to the water level and make sure that the level is kept not so high as to lead to core melt-down. The definition of this event is the operator fails to complete this job.*
long-term heat removal	W	HFD	v_{10}	*The residual heat removal (RHR) system is initialized to cool down the suppression pool and containment in order to maintain other supporting systems work well. If this system fails, event W will happen.*
vessel inventory makeup after containment (CTMT) failure	V_W	HFD	v_{11}	*The CTMT might fail because of over-pressure or over-heat. The water in the reactor vessel must be kept supplying to protect the fuel not to be melt in the condition of CTMT failure. Among these events, X_I, X_C and X_V are mainly caused by human errors. The others are mainly caused by hardware failures.*

Table A2. Parameters of the Probability Density Functions [31]

event	pdf	median	error factor
T1ACM	$p_{v1}(v)$	1.52E-07	8.42
R	$p_{v2}(v)$	1.96E-03	5.00
M	$p_{v3}(v)$	1.00E-05	5.00
C_0	$p_{v4}(v)$	1.37E-02	3.00
U1	$p_{v5}(v)$	8.45E-02	3.00
U	$p_{v6}(v)$	2.13E-03	5.00
V1	$p_{v7}(v)$	1.12E-06	10.00
V2	$p_{v8}(v)$	3.40E-06	10.00
V3	$p_{v9}(v)$	9.49E-05	10.00
W	$p_{v10}(v)$	2.03E-05	10.00
V_W	$p_{v11}(v)$	4.00E-01	2.40

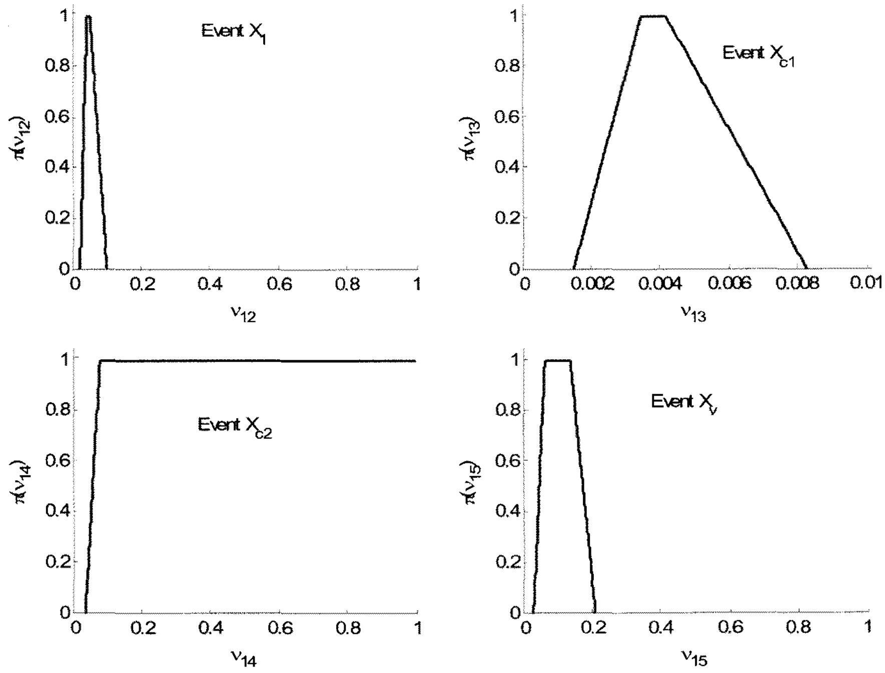

Fig A1. Possibility Distributions of the Probabilities of Occurrence of the Four Human-Error-Dominated Events of the Event Tree of Fig 3 [31]