Rakowsky Uwe Kay
University of Wuppertal, Germany, and Vossloh Kiepe, Düsseldorf, Germany

Fundamentals of the Dempster-Shafer theory and its applications to system safety and reliability modelling

Keywords

Dempster-Shafer Theory, evidence, uncertainty, expert assessment, Event Tress Analysis, Fault Tree Analysis

Abstract

The Dempster-Shafter Theory is well-known for its usefulness to express uncertain judgments of experts. This contribution shows how to apply the calculus to safety and reliability modelling, especially to expert judgement; Failure Modes, Effects, and Criticality Analysis; Event Tree Analysis, Fault Tree Analysis, and Reliability Centred Maintenance. Including a tutorial introduction to the Dempster-Shafer Theory, the differences between the Probability and the Dempster-Shafer Theory are discussed widely.

1. Introduction

In the middle of the 1960s Arthur P. Dempster developed a theory [1], [2], [3] that includes a kind of "upper and lower probabilities". Later, it turned out that this approach is very useful to express uncertain judgments of experts.

About ten years later the work of Dempster was extended, refined, recast, and published by Glenn Shafer [18] as a "Mathematical Theory of Evidence". Shafer e.g. rebuilt the mathematical theory around the Dempster concept and introduced degrees of belief instead of lower probabilities. The Theory of Evidence was also denoted as the *Dempster-Shafer Theory* (DST) or the *Dempster-Shafer Evidential Theory*.

The more the *Dempster-Shafer Theory* was further developed, the more the evidence measures of DST departed from being probabilities, e.g. Klir & Folger [11] revised DST in that sense. As stated by [4] and [20], the advantage of DST is that it allows coping with absence of preference, due to limitations of the available information, which results in indeterminacy.

2. Fundamentals

The DST became known to the safety and reliability community in the early 1990s, refer e.g. Guth [7]. The reliability-oriented approach to DST as presented here is based on a *scenario* that contains the system with all hypotheses, pieces of evidence and data sources.

The *hypotheses* represent all the possible states (e.g. faults) of the system considered. It is required that all hypotheses are elements (singletons) of the *frame of discernment*, which is given by the finite universal set Ω. The set of all subsets of Ω is its power set 2^{Ω}. A subset of those 2^{Ω} sets may consist of a single hypothesis or of a conjunction of hypotheses. Moreover, it is required that all hypotheses are unique, not overlapping and mutually exclusive.

In this context *pieces of evidence* are symptoms or events (e.g. failures) that occurred or may occur within a system. One piece of evidence is related to a single hypothesis or a set of hypotheses. It is not allowed that different pieces of evidence lead to the same hypothesis or set of hypotheses.

The qualitative relation between a piece of evidence and a hypothesis corresponds to a cause-consequence chain: A piece of evidence implies a hypothesis or a set of hypotheses, respectively. The strength of an evidence-hypothesis assignment, and thereby the strength of this implication, is quantified by a statement of a data source.

Data sources are persons, organisations, or any other entities that provide information for a scenario. In safety and reliability engineering, data sources are usually the results of empirical studies or they are experts, who give subjective quantifiable statements. As required by O'Neill [13], data sources have to be representative (e.g. studies) or as free from bias as possible (e.g. experts).

Some misunderstandings in interpretations concerning the plot of hypotheses have to be cleared up. From an objective point of view, which might e.g. be located outside the system (e.g. observer), exactly one single hypothesis is true; from a subjective point of view of a data source (e.g. expert or operator), it might be uncertain which hypothesis fits best to reality. Therefore, DST makes it possible to model several

- single pieces of evidence within single hypothesis relations or
- single pieces of evidence within multi hypotheses relations

as uncertain assessments of a system in which exactly one hypothesis is objectively true. Both points of view, the objective and the subjective, have to be distinguished clearly. The DST calculus describes the subjective viewpoint as an assessment for an unknown objective fact.

By means of a data source, a mapping

$$m\colon 2^{\Omega} \rightarrow [0, 1] \tag{1}$$

assigns an evidential weight to a set $\boldsymbol{A} \subseteq \Omega$, which contains a single hypothesis or a set of hypotheses. This is the most significant difference to the Probability Theory: The DST mapping distinguishes clearly between the evidence measures and probabilities with mapping $\Omega \rightarrow [0, 1]$. Each $\boldsymbol{A}$ that holds $m(\boldsymbol{A}) > 0$ is called a focal element. The function m is called a *basic assignment* and fulfils

$$\textstyle\sum_{\boldsymbol{A}\subseteq\Omega} m(\boldsymbol{A}) = 1 \ . \tag{2}$$

This equation means that all statements of a single data source have to be normalised, just to ensure that the evidence presented by each data source is equal in weight, e.g. no data source is more important than another one. – For the "sake of simplicity" (Klir & Folger [11]), it is assumed that

$$m(\varnothing) = 0 \ ; \tag{3}$$

however, this property requires an appropriate choice of the universal set Ω. That means, the set Ω has to be complete and contain all possible hypotheses of the scenario considered.

In some publications m is called the *basic probability assignment*, refer Shafer [18], which misleads to the assumption $m(\boldsymbol{A})$ might be a probability. Further denotations are the *basic belief assignment* [19], the *belief structure* [21], [4] or the *mass assignment function* [14].

A clear distinction has to be made between probabilities and basic belief assignment: probability distribution functions are defined on Ω and basic assignment functions on the power set 2^{Ω}. In addition, m has three further properties, which distinguishes it from being a probability function, refer Klir & Folger [11]: It is not required

- that $m(\Omega) = 1$,
- that $m(\boldsymbol{A}) \leq m(\boldsymbol{B})$ if $\boldsymbol{A} \subset \boldsymbol{B}$, or
- that there is a relationship between $m(\boldsymbol{A})$ and $m(\neg\boldsymbol{A})$.

Therefore, it seems to be useful to avoid the terms *probability* and *belief* (which is defined next) in the denotation of m.

By applying the *basic assignment function*, several *evidential functions* can be created. A *belief measure* is given by the function $bel\colon 2^{\Omega} \rightarrow [0,1]$. There is

$$bel(\boldsymbol{A}) = \textstyle\sum_{B\subseteq A;B\neq\phi} m(\boldsymbol{B}) \,. \tag{4}$$

The counterpart of *bel* is the plausibility measure pl: $2^{\Omega} \rightarrow [0,1]$ with

$$pl(\boldsymbol{A}) = \textstyle\sum_{B\cap A\neq\phi} m(\boldsymbol{B}) \,. \tag{5}$$

The measure $pl(\boldsymbol{A})$ shall not be understood as the complement of $bel(\boldsymbol{A})$. Only

$$\{\boldsymbol{A} \subseteq \Omega \mid m(\boldsymbol{A}) > 0\} \neq \varnothing \rightarrow bel(\boldsymbol{A}) \leq pl(\boldsymbol{A}) \tag{6}$$

has to be fulfilled. In addition to *bel* and *pl*, a third evidential function can be defined. Shafer [18] introduced the *commonality measure* with $cmn\colon 2^{\Omega} \rightarrow [0,1]$ and

$$cmn(\boldsymbol{A}) = \textstyle\sum_{B\supseteq A} m(\boldsymbol{B}) \,. \tag{7}$$

Figure 1 shows a graphical representation of the above-defined measures *belief* and *plausibility*. The difference $pl(\boldsymbol{A}) - bel(\boldsymbol{A})$ describes the evidential interval range, which represents the uncertainty concerning the set $\boldsymbol{A}$.

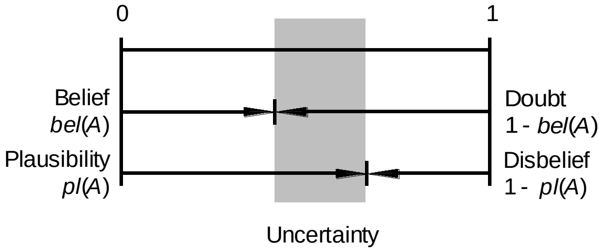

Figure 1. Measures of belief and plausibility and its complements for a given bel(**A**) < pl(**A**). The evidential or the uncertainty interval, respectively, is shaded grey.

The complements to the measures *belief* and *plausibility* are *doubt* and *disbelief*, respectively. Although Shafer ([18], page 43) defines *doubt* as a complement to the measure plausibility, it seems to make more sense to distinguish between *doubt* and *disbelief* in the way given above because DST does not require a causal relationship between a hypothesis and its negation. As Flack [6] emphasises, lack of *belief* does not imply *disbelief*. The *disbelief* of set $\underline{\boldsymbol{A}}$ is the belief in the complement. There is

$$bel(\neg \boldsymbol{A}) = 1 - pl(\boldsymbol{A})\ ,\ pl(\neg \boldsymbol{A}) = 1 - bel(\boldsymbol{A}) \qquad (8)$$

with

$$bel(\neg \boldsymbol{A}) \le pl(\neg \boldsymbol{A})\ . \qquad (9)$$

The difference $pl(\boldsymbol{A}) - bel(\boldsymbol{A})$ describes the *uncertainty* concerning the hypothesis ***A*** represented by the evidential interval, see *Figure 1*.

2.1. Interpretations on Evidence Measures

Some helpful and interesting interpretations of the evidence measures are given in the literature and cited here.

Basic Assignment

- The measure $m(\boldsymbol{A})$ assigns an evidential weight to the set ***A***, refer Flack [6].
- The measure $m(\boldsymbol{A})$ is the degree of evidence that the element in question belongs exactly to the set ***A***, refer Klir & Folger [11].
- The measure $m(\boldsymbol{A})$ is the degree of evidence supporting the claim that a specific element of Ω belongs to the set ***A***, but not to any special subset of ***A***, refer Klir & Folger [11].
- The quantity $m(\boldsymbol{A})$ is the degree of belief that the above specified claim is warranted, refer Klir & Folger [11].

Belief

- The measure $bel(\boldsymbol{A})$ is the degree of evidence that the element in question belongs to the set ***A*** as well as to the various special subsets of ***A***, refer Klir & Folger [11].
- The measure $bel(\boldsymbol{A})$ can be interpreted as the total amount of justified support given to ***A***, refer Denoeux [4].
- The measure $bel(\boldsymbol{A})$ is the degree of evidence supporting the claim that a specific element of Ω belongs to the set ***A***, but not to any special subset of ***A***, refer Klir & Folger [11].

Plausibility

- The quantity $pl(\boldsymbol{A})$ is the degree of evidence that the element in question belongs to the set ***A*** or to any of its subsets [or to any set that overlaps with **A**], refer Klir & Folger [11].
- The quantity $pl(\boldsymbol{A})$ can be interpreted as the maximum amount of specific support that could be given to ***A***, if justified by additional information, refer Smets [19].

2.2. Bayesian Statistical Modelling versus Dempster-Shafer Theory

Flack [6] describes the differences between the *Bayesian statistical modelling* and the *Dempster-Shafer Theory* as a difference in concepts. A Bayesian model describes a Boolean type of phenomena, which either exist or do not exist. Little belief in the existence of a phenomenon implies a strong belief in its non-existence. This implication does not necessarily hold for DST. Here, no causal relationship is required between both, belief in existence and belief in non-existence. For example, a statement concerning the failure probability of an item also implies a statement about its counterpart, the reliability of the same item. DST does not require this sub-proposition; and that adds new aspects and possibilities to reliability modelling.

As stated by Ferson et al. [5], the Dempster-Shafer Theory has been widely studied in computer science and artificial intelligence, but has never achieved complete acceptance among probabilists and traditional statisticians. (By this, the question arises if any other theory than the Probability Theory would ever be accepted by probabilists or traditional statisticians.)

However, there are still some disadvantages of the Probability Theory for the DST, which should also be stated here. There are three undesired main properties as listed by [4]:

- *Lack of introspection or assessment strategies*: The main criticisms of the Bayesian statistical modelling is its unreasonable requirement for precision. But the necessity to assign precise numbers in DST applications to each subset $\boldsymbol{A} \subseteq \Omega$ by the basic assignment m is constraining in the same way. Precise degrees of the desired measures may exist, but it is perhaps too difficult to determine them with the necessary precision.
- *Instability*: Underlying beliefs may be unstable. Estimated beliefs may be influenced by the conditions of its estimation.
- *Ambiguity*: Ambiguous or imprecise judgement could not be expressed by the evidence measures.

Additional statements to disadvantages of the Dempster-Shafer Theory are:

- DST lists all the hypotheses into the frame of discernment Ω, which resembles the fault space in the Bayesian Theory. However, given k hypotheses, it can consist of up to 2^k elements, representing all possible subsets of Ω. This leads to a similar problem encountered in the Bayesian Theory, except that it is worse because human experts have to estimate a larger number of belief values than after the Bayesian theory [12].

- Another caveat of the applicability of DST is that it does not offer a procedure for implementation of a diagnostic system [10].

2.3. Dempster-Shafer Rule of Combination

Dempster [2], [3] followed by Shafer [18] suggested a rule of combination which allows that the basic assignments are combined. There is

$$m(\boldsymbol{Z}) = \frac{\sum\limits_{\boldsymbol{A}\cap\boldsymbol{B}=\boldsymbol{Z}\neq\phi} m(\boldsymbol{A})\cdot m(\boldsymbol{B})}{1-\sum\limits_{\boldsymbol{A}\cap\boldsymbol{B}=\phi} m(\boldsymbol{A})\cdot m(\boldsymbol{B})}, \tag{10}$$

with $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{Z} \subseteq \Omega$. Verbally: the numerator represents the accumulated evidence for the sets $\boldsymbol{A}$ and $\boldsymbol{B}$, which supports the hypothesis $\boldsymbol{Z}$, and the denominator sum quantifies the amount of conflict between the two sets. Depending on the application, the denominator of

$$m(\boldsymbol{Z}) = \frac{\sum\limits_{\boldsymbol{A}\cap\boldsymbol{B}=\boldsymbol{Z}\neq\phi} m(\boldsymbol{A})\cdot m(\boldsymbol{B})}{\sum\limits_{\boldsymbol{A}\cap\boldsymbol{B}\neq\phi} m(\boldsymbol{A})\cdot m(\boldsymbol{B})}, \tag{11}$$

is easier to apply.

3. Illustration

The following illustration is strictly step-wise structured and gives an easy-to-understand introduction to the calculus of the Dempster-Shafer Theory.

The given scenario discusses a typical situation in a power plant. The operators at the control panel detect serious changes of the system properties. Some failures are detectable; however, their consequences or the system fault, respectively, can neither be determined exactly nor interpreted certainly. (This situation is widely discussed e.g. in the ATHEANA Report [14] and by Hollnagel [8].) To avoid an error forcing context, pieces of evidence are collected, hypotheses are postulated, and conclusions are made on this basis. Therefore, a Dempster-Shafer approach is applied to support the operators in decision making.

Step ❶ – *Creating the Scenario*

The scenario consists of a power plant (the system considered), two operators (data sources, denoted by the index *l*), the failures detected (pieces of evidence), and the system fault states (set of hypotheses). As described above, the pieces of evidence correspond to *failures* or *causes* and the hypotheses to *faults* or *consequences*.

The faults can be determined to at most three precisely defined hypotheses represented by the set Ω with

$$\Omega = \{h_1, h_2, h_3\} \; . \tag{12}$$

With that, the frame of discernment of this context is given. It should be noted that Ω is postulated by the operators based on their subjective points of view, assuming that Ω is complete. The corresponding power set of Ω is

$$2^{\Omega} = \{\varnothing, \{h_1\}, \{h_2\}, \{h_3\}, \{h_1, h_2\}, \{h_1, h_3\}, \{h_2, h_3\}, \Omega\} \; . \tag{13}$$

The first operator mainly states that the faults h_1 or h_2 are the reason for the problems. For example, the failure ev_3 might have occurred and resulted in the consequences h_1 or h_2. The assignments of the second operator are slightly different. Here, focus is on the faults h_1 or h_3. Both operators give their statements to the four pieces of evidence found. The complete survey of the qualitative failure-fault(s) assignments is given in *Table 1.*

Table 1. Qualitative failure-fault(s) assignments given by the operators involved

		Failure	Fault(s)
Operator	1st	ev_1	h_1
		ev_2	h_2
		ev_3	h_1, h_2
		ev_4	h_1, h_2, h_3
	2nd	ev_1	h_1
		ev_2	h_3
		ev_3	h_1, h_3
		ev_4	h_1, h_2, h_3

Please note that contrary to the *Fault Tree Analysis* (FTA), DST does not allow that more than one failure lead to the same fault (hypothesis). However, different failures may have different set of consequences, which may contain the same hypotheses as elements, e.g. ev_1, ev_3, and ev_4 in *Table 1* lead to hypotheses, which all contain h_1 as a fault. Again, DST allows modelling several

- *single*-failure-*single*-fault relations and
- *single*-failure-*multi*-fault relations

as an uncertain assessment of a system, which can take exactly one state at a time. Generally, DST emphasizes more on the hypotheses (faults) than on the pieces of evidence (failures), which are of minor interest in the next steps.

As described in Section 0, the system is exactly in one state of Ω. In other words, exactly one hypothesis of $\{h_1, h_2, h_3\}$ is true for the given scenario and situation if the system would be observed from an objective point of view. Subjectively, the operators are not sure, in which state the system actually is.

Step ❷ – *Quantification of Statements*

At this step, both operators quantify their statements as given in Table 2. The set of hypotheses ***A*** is assigned to the first operator, ***B*** to the second operator. For example, the second operator claims that the consequences h_1 or h_3 may have occurred with a basic assignment of 0.4. (Formulating this sentence verbally, it is rather difficult to avoid that the tongue mentions “probability”. Again, basic assignments are not probabilities, see equation (1).) Non-specified statements are assigned by 0 and are not focal elements.

The subjective quantifications of the operators are based on their system experiences and mostly on their “engineering feelings”. Certainly, these quantifications are imprecise.

Table 2. Quantitative statements given by the operators involved (outer columns). The inner column contains all subsets of the power set $2^{\square}$.

1st operator	2^{Ω}	2nd operator
$m(\boldsymbol{A}_1) = 0.2$	$\{h_1\}$	$m(\boldsymbol{B}_1) = 0.2$
$m(\boldsymbol{A}_2) = 0.1$	$\{h_2\}$	$m(\boldsymbol{B}_2) = 0$
$m(\boldsymbol{A}_3) = 0$	$\{h_3\}$	$m(\boldsymbol{B}_3) = 0.2$
$m(\boldsymbol{A}_4) = 0.6$	$\{h_1 \cup h_2\}$	$m(\boldsymbol{B}_4) = 0$
$m(\boldsymbol{A}_5) = 0$	$\{h_1 \cup h_3\}$	$m(\boldsymbol{B}_5) = 0.4$
$m(\boldsymbol{A}_6) = 0$	$\{h_2 \cup h_3\}$	$m(\boldsymbol{B}_6) = 0$
$m(\boldsymbol{A}_7) = 0.1$	$\{h_1 \cup h_2 \cup h_3\}$	$m(\boldsymbol{B}_7) = 0.2$

Based on the basic assignments given by both operators, the *belief* and *doubt*, *commonality*, *plausibility* and *disbelief* measures can be calculated. For example, the *belief* in the set of hypotheses $\{h_1 \cup h_2\}$ is the sum of its own basic assignment with those of all of its subsets

$$\{h_1\}, \{ h_2\}, \{h_1 \cup h_2\} \subseteq \{h_1 \cup h_2\} \, , \tag{14}$$

see equation (4). For the fourth statement of the first operator there is

$$bel(\boldsymbol{A}_4) = m(\boldsymbol{A}_1) + m(\boldsymbol{A}_2) + m(\boldsymbol{A}_4) = 0.9, \tag{15}$$

with the corresponding *doubt* measure

$$1 - bel(\boldsymbol{A}_4) = 0.1 \, . \tag{16}$$

The *commonality* takes every statement into account, which includes the discussed statement completely. There is for $\boldsymbol{A}_4$

$$\{h_1 \cup h_2\}, \{ h_1 \cup h_2 \cup h_3\} \supseteq \{h_1 \cup h_2\} \, , \tag{17}$$

$$cmn(\boldsymbol{A}_4) = m(\boldsymbol{A}_4) + m(\boldsymbol{A}_7) = 0.7 \, . \tag{18}$$

The *plausibility* includes basic assignments of all statements which have got at least one hypothesis with those of the discussed statement in common. Concerning $\boldsymbol{A}_4$, there is

$$\begin{gathered}\{h_1\}, \{h_2\}, \{h_1 \cup h_2\}, \{h_1 \cup h_3\}, \{h_2 \cup h_3\}, \\ \{h_1 \cup h_2 \cup h_3\} \cap \{h_1 \cup h_2\} \neq \varnothing \, ,\end{gathered} \tag{19}$$

which results in the *plausibility*

$$\begin{aligned} pl(\boldsymbol{A}_4) &= m(\boldsymbol{A}_1) + m(\boldsymbol{A}_2) + m(\boldsymbol{A}_4) + m(\boldsymbol{A}_5) \\ &\quad + m(\boldsymbol{A}_6) + m(\boldsymbol{A}_7) = 1 \end{aligned} \tag{20}$$

and finally in no *disbelief* at all

$$1 - pl(\boldsymbol{A}_4) = 0 \, . \tag{21}$$

Table 3 shows the results for *belief* and *plausibility* of all statements ($k = 1,\ldots, 7$).

Table 3. This table corresponds to *Table 2* and shows the values of basic assignments (bold typing), belief, and plausibility for each statement and operator (first left side, second right side).

$m(A_k)$	$bel(A_k)$	$pl(A_k)$	2^{Ω}	$m(B_k)$	$bel(B_k)$	$pl(B_k)$
0.2	0.2	0.9	$\{h_1\}$	**0.2**	0.2	0.8
0.1	0.1	0.8	$\{h_2\}$	**0**	0	0.2
0	0	0.1	$\{h_3\}$	**0.2**	0.2	0.8
0.6	0.9	1	$\{h_1 \cup h_2\}$	**0**	0.2	0.8
0	0.2	0.9	$\{h_1 \cup h_3\}$	**0.4**	0.8	1
0	0.1	0.8	$\{h_2 \cup h_3\}$	**0**	0.2	0.8
0.1	1	1	Ω	**0.2**	1	1

Step ❸ – *Combining Hypotheses*

The third step combines each hypothesis or set of hypotheses, respectively, from one data source (operator) with one from the other source and builds the cut set of both, see *Table 4*. Depending on quantifications given at Step ❷, some of the cut sets may not be focal elements before or thereafter. Actually, this step was fit in for illustrative purpose and can be combined with Step ❹.

Table 4. The Combination Table contains the full plot of hypotheses cut sets of $\boldsymbol{A}$ and $\boldsymbol{B}$

$\cap$	$\boldsymbol{A}_1$	$\boldsymbol{A}_2$	$\boldsymbol{A}_3$	$\boldsymbol{A}_4$	$\boldsymbol{A}_5$	$\boldsymbol{A}_6$	$\boldsymbol{A}_7$
$\boldsymbol{B}_1$	h_1	$\varnothing$	$\varnothing$	h_1	h_1	$\varnothing$	h_1
$\boldsymbol{B}_2$	$\varnothing$	h_2	$\varnothing$	h_2	$\varnothing$	h_2	h_2
$\boldsymbol{B}_3$	$\varnothing$	$\varnothing$	h_3	$\varnothing$	h_3	h_3	h_3
$\boldsymbol{B}_4$	h_1	h_2	$\varnothing$	$h_1 \cup h_2$	h_1	h_2	$h_1 \cup h_2$
$\boldsymbol{B}_5$	h_1	$\varnothing$	h_3	h_1	$h_1 \cup h_3$	h_3	$h_1 \cup h_3$
$\boldsymbol{B}_6$	$\varnothing$	h_2	h_3	h_2	h_3	$h_2 \cup h_3$	$h_2 \cup h_3$
$\boldsymbol{B}_7$	h_1	h_2	h_3	$h_1 \cup h_2$	$h_1 \cup h_3$	$h_2 \cup h_3$	Ω

Step ❹ – *Reducing the Combination Table*

To avoid mathematical effort, those columns and rows of the Combination *Table 4* were dropped, which are related to non-focal elements (non-specified statements with $m(\boldsymbol{A}_k) = 0$, $m(\boldsymbol{B}_k) = 0$). In this context, columns $\boldsymbol{A}_3$, $\boldsymbol{A}_5$, $\boldsymbol{A}_6$ and rows $\boldsymbol{B}_2$, $\boldsymbol{B}_4$, $\boldsymbol{B}_6$ are not applicable. *Table 5* shows the reduced plot containing the combinations of focal elements exclusively.

Table 5. The reduced Combination Table

$\cap$	$\boldsymbol{A}_1$	$\boldsymbol{A}_2$	$\boldsymbol{A}_4$	$\boldsymbol{A}_7$
$\boldsymbol{B}_1$	h_1	$\varnothing$	h_1	h_1
$\boldsymbol{B}_3$	$\varnothing$	$\varnothing$	$\varnothing$	h_3
$\boldsymbol{B}_5$	h_1	$\varnothing$	h_1	$h_1 \cup h_3$
$\boldsymbol{B}_7$	h_1	h_2	$h_1 \cup h_2$	Ω

Step ❺ – *Calculating Products and Sums of Combined Basic Assignments*

At this step, products of the related basic assignments are calculated from the non-empty sets. Products of basic assignments corresponding to the same cut set have to be added. For $\{h_1\}$ yields

$$\boldsymbol{Z}_1 = \boldsymbol{A}_1 \cap \boldsymbol{B}_1 = \{h_1\}$$

$$\Rightarrow m(\boldsymbol{Z}_1) = m(\boldsymbol{A}_1) \cdot m(\boldsymbol{B}_1) = 0.04\ , \tag{22}$$

$$\boldsymbol{Z}_2 = \boldsymbol{A}_1 \cap \boldsymbol{B}_5 = \{h_1\}$$

$$\Rightarrow m(\boldsymbol{Z}_2) = m(\boldsymbol{A}_1) \cdot m(\boldsymbol{B}_5) = 0.08\ , \tag{23}$$

$$\boldsymbol{Z}_3 = \boldsymbol{A}_1 \cap \boldsymbol{B}_7 = \{h_1\}$$

$$\Rightarrow m(\boldsymbol{Z}_3) = m(\boldsymbol{A}_1) \cdot m(\boldsymbol{B}_7) = 0.04\ , \tag{24}$$

$$\boldsymbol{Z}_4 = \boldsymbol{A}_4 \cap \boldsymbol{B}_1 = \{h_1\}$$

$$\Rightarrow m(\boldsymbol{Z}_4) = m(\boldsymbol{A}_4) \cdot m(\boldsymbol{B}_1) = 0.12\ , \tag{25}$$

$$\boldsymbol{Z}_5 = \boldsymbol{A}_4 \cap \boldsymbol{B}_5 = \{h_1\}$$

$$\Rightarrow m(\boldsymbol{Z}_5) = m(\boldsymbol{A}_4) \cdot m(\boldsymbol{B}_5) = 0.24\ , \tag{26}$$

$$\boldsymbol{Z}_6 = \boldsymbol{A}_7 \cap \boldsymbol{B}_1 = \{h_1\}$$

$$\Rightarrow m(\boldsymbol{Z}_6) = m(\boldsymbol{A}_7) \cdot m(\boldsymbol{B}_1) = 0.02 \tag{27}$$

with the sum

$$\sum_{k=1}^{6} m(\boldsymbol{Z}_k) = 0.54\,. \tag{28}$$

Hypotheses h_2 or h_3 are supported by

$$\boldsymbol{Z}_7 = \boldsymbol{A}_2 \cap \boldsymbol{B}_7 = \{h_2\}$$

$$\Rightarrow m(\boldsymbol{Z}_7) = m(\boldsymbol{A}_2) \cdot m(\boldsymbol{B}_7) = 0.02\ , \tag{29}$$

$$\boldsymbol{Z}_8 = \boldsymbol{A}_7 \cap \boldsymbol{B}_3 = \{h_3\}$$

$$\Rightarrow m(\boldsymbol{Z}_8) = m(\boldsymbol{A}_7) \cdot m(\boldsymbol{B}_3) = 0.02\ . \tag{30}$$

There is for the sets $\{h_1 \cup h_2\}$, $\{h_1 \cup h_3\}$, and $\{h_1 \cup h_2 \cup h_3\}$:

$$\boldsymbol{Z}_9 = \boldsymbol{A}_4 \cap \boldsymbol{B}_7 = \{h_1 \cup h_2\}$$

$$\Rightarrow m(\boldsymbol{Z}_9) = m(\boldsymbol{A}_4) \cdot m(\boldsymbol{B}_7) = 0.12\ , \tag{31}$$

$$\boldsymbol{Z}_{10} = \boldsymbol{A}_7 \cap \boldsymbol{B}_5 = \{h_1 \cup h_3\}$$

$$\Rightarrow m(\boldsymbol{Z}_{10}) = m(\boldsymbol{A}_7) \cdot m(\boldsymbol{B}_5) = 0.04\ , \tag{32}$$

$$\boldsymbol{Z}_{11} = \boldsymbol{A}_7 \cap \boldsymbol{B}_7 = \{h_1 \cup h_2 \cup h_3\}$$

$$\Rightarrow m(\boldsymbol{Z}_{11}) = m(\boldsymbol{A}_7) \cdot m(\boldsymbol{B}_7) = 0.02\ . \tag{33}$$

To illustrate this formal procedure, the results are given in *Table 6*.

Table 6. This table corresponds directly to *Table 5* and represents the products (•) of basic assignments; ✖ means *no focal element*

•	$\boldsymbol{A}_1$	$\boldsymbol{A}_2$	$\boldsymbol{A}_4$	$\boldsymbol{A}_7$
$\boldsymbol{B}_1$	0.04	✖	0.12	0.02
$\boldsymbol{B}_3$	✖	✖	✖	0.02
$\boldsymbol{B}_5$	0.08	✖	0.24	0.04
$\boldsymbol{B}_7$	0.04	0.02	0.12	0.02

Step ❻ – *Combining Basic Assignments*

The sum over all combinations calculated in Step ❺,

$$\sum_{k=1}^{11} m(\boldsymbol{Z}_k) = 0.76\,. \tag{34}$$

is identical with the denominator of equation (11). With that, the basic assignment of every hypothesis can be calculated. There is

$$m(\{h_1\}) = \frac{\sum_{k=1}^{6} m(\boldsymbol{Z}_k)}{\sum_{k=1}^{11} m(\boldsymbol{Z}_k)} \approx 0.7105 \tag{35}$$

for the hypothesis h_1 and

$$m(\{h_2\}) = \frac{m(\boldsymbol{Z}_7)}{\sum_{k=1}^{11} m(\boldsymbol{Z}_k)} \approx 0.0263 \tag{36}$$

$$m(\{h_3\}) = \frac{m(\boldsymbol{Z}_8)}{\sum_{k=1}^{11} m(\boldsymbol{Z}_k)} \approx 0.0263 \tag{37}$$

$$m(\{h_1 \cup h_2\}) = \frac{m(\boldsymbol{Z}_9)}{\sum_{k=1}^{11} m(\boldsymbol{Z}_k)} \approx 0.1579 \tag{38}$$

$$m(\{h_1 \cup h_3\}) = \frac{m(\boldsymbol{Z}_{10})}{\sum_{k=1}^{11} m(\boldsymbol{Z}_k)} \approx 0.0526 \tag{39}$$

$$m(\{h_1 \cup h_2 \cup h_3\}) = \frac{m(\boldsymbol{Z}_{11})}{\sum_{k=1}^{11} m(\boldsymbol{Z}_k)} \approx 0.0263 \tag{40}$$

for all relevant sets of hypotheses.

Step ❼ – Evidence Measures of Combined Hypotheses

The evidence measures of combined hypotheses are calculated according to Step ❶, *Table 7*. The set $\{h_1 \cup h_2\}$ does not occur because it vanished in *Table 5*.

Step ❽ – *Interpretation*

Starting at the same low value, h_3 takes roughly half the range of uncertainty that h_2 takes. However, both hypotheses alone should not be considered further due to the low values of belief and plausibility. With about ~0.24, the single hypothesis h_1 is assigned with a wide range of uncertainty. The combination of h_1 and h_3 covers a smaller range (~0.18) than h_1 alone, and it has a higher plausibility. Finally, a combination of h_1 and h_2 shows the smallest range of uncertainty (~0.08) with the same (highest) plausibility as in case of the combination of h_1 and h_3.

The conclusion is that a combination of h_1 and h_2 may be responsible for the serious changes of the system properties. Please note that a probabilistic approach would have blamed h_1 alone for being responsible. (And please consider the consequences.) This result clearly shows the differences between both theories, based on their different mappings Ω → [0, 1] versus 2^{Ω} → [0, 1], see Section 0.

Table 7. The *basic assignments* (bold) and the resulting evidence measures *belief*, *commonality*, and *plausibility* are given; hypotheses are ranked by their belief measures, all values are rounded.

2^{Ω}	*m*	*bel*	*cmn*	*pl*
Ω	**0.0263**	1	0.0263	1
$\{h_1 \cup h_2\}$	**0.1579**	0.8947	0.1842	0.9737
$\{h_1 \cup h_3\}$	**0.0526**	0.7895	0.0789	0.9737
$\{h_1\}$	**0.7105**	0.7105	0.9474	0.9471
$\{h_2\}$	**0.0263**	0.0263	0.2105	0.2105
$\{h_3\}$	**0.0263**	0.0263	0.1053	0.1053

4. Applications to System Safety and Reliability Modelling

The introductory descriptions of the *Failure Modes, Effects, and Criticality Analysis*, the *Event Tree Analysis*, and the *Fault Tree Analysis* are taken from the "System Safety Analysis Handbook" written by Stephens & Talso [29] and published by the *System Safety Society*. The descriptions are shortened and slightly revised. The introductory description of the Reliability Centred Maintenance is taken from [23]. Additionally, the IEC standards are recommended for the application of all listed methods, refer to Section 0.

4.1. Failure Modes, Effects, and Criticality Analysis

As described by Stephens & Talso [29], the *Failure Modes, Effects, and Criticality Analysis* (FMECA) tabulates a list of items in a process along with all the possible failure modes for each item. The effect of each failure is evaluated and ranked according to a severity classification. An FMECA includes the following steps:

- Define the worksheet formats and ground rules.
- Give analysis assumptions.
- Identify the lowest indenture level of analysis.
- Code the system description.
- Give failure definitions and evaluations.

The usefulness of the FMECA as a design tool and in the decision making process depends on the effectiveness with which problem information is communicated for early design attention. Probably the most severe criticism of the FMECA has been its limited use for improvement of designs, as Stephens & Talso [29] claim. The main causes for this have been the untimeliness and the isolated performance of the FMECA without adequate inputs to the design process. While the objective of an FMECA is to identify all modes of failure within a system design, its first purpose is the early identification of all critical failure probabilities so that they can be eliminated or minimised through design correction at the earliest possible time.

The Dempster-Shafer calculus, as described by the illustration in Section 0, can easily be applied to the FMECA. If more than one expert is involved in the quantitative assessments of the criticality and the occurrence of an item failure. The results are narrow or wide ranges of uncertainties, which require an interpretation similar to Step ❽ Section 0.

However, it is an interesting question if institutions, which conduct system homologations, would accept these results.

4.2. Event Tree Analysis

As summarised by Stephens & Talso [29], the *Event Tree Analysis* (ETA) is an analytical tool that can be used to organise, characterise, and quantify potential failures in a methodical manner. An event tree models the sequence of events that results from a single initiating event. The ETA is a bottom-up analysis versus the top-down approach for the Fault Tree Analysis, see Section 0.

Conducting an ETA starts with selection of the initiating events, both the desired events and the ones not desired. Thereafter, their consequences are developed through consideration of component, module, and system failure-and-success alternatives, respectively. The identification of initiating events may be based on review of the system design and operation, the results of another safety analysis, or personal operating experience acquired with a similar system. Then the success and failure of the mitigating systems are postulated and continued through all alternate paths, considering each consequence as a new initiating event. The basic steps for construction of an event tree include the following:

- List all possible initiating events.
- Identify functional system responses.
- Identify support system responses.
- Group initiating events with all responses.
- Define failure sequences.
- Assign probabilities to each step in the event tree to arrive at total probability of occurrence for each failure sequence.

The method is universally applicable to all kinds of systems, with the limitation that all events must be anticipated to produce meaningful analytical results.

Among the methods presented in the “System Safety Analysis Handbook” by Stephens & Talso [29], the *Event Tree Analysis* is definitely one of the most exhaustive, if it is applied properly. Axiomatically, their use also consumes large quantities of resources. Their use, therefore, is well reserved for systems in which risks are regarded as high and well concealed.

As described by Stephens & Talso [29], probabilities are assigned to each step in the event tree. To apply evidence measures instead of probabilities, the following steps are conducted, which lead to the *Dempster-Shafer Event Tree Analysis DS*-ETA.

It is assumed that the considered event tree consists of bifurcations only; i.e., any symbol within an event tree has one input and two outputs (the event “failure” or the event “no failure”), see *Figure 2.*

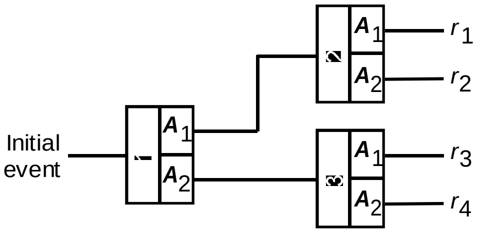

Figure 2. Event tree with three bifurcations resulting in four sequences, $\boldsymbol{A}_1$ denotes “failure” and $\boldsymbol{A}_2$ “no failure”

Every bifurcation $i = 1, \ldots, n$ of an event tree is considered separately and independently from the $n - 1$ other bifurcations. The assigned set of hypotheses contains $\Omega_i = \{\boldsymbol{A}_1, \boldsymbol{A}_2, \boldsymbol{A}_3\} \equiv$ {“failure”, “no failure”, “uncertain”}. Hence, any expert (data source) l has to give three values for the basic assignments $m_{l,i}(\boldsymbol{A}_k)$, $k = 1, 2, 3$ of any bifurcation i, representing his/her degree of belief that $\boldsymbol{A}_k$ may occur. Obviously, the uncertainty of an expert concerning an event $\boldsymbol{A}_3$ does not appear in the graphical representation. There is for the *Expert Assessment Matrix*

$$\boldsymbol{M}_l = \begin{bmatrix} m_{l,1}(\boldsymbol{A}_1) & m_{l,1}(\boldsymbol{A}_2) & m_{l,1}(\boldsymbol{A}_3) \\ \vdots & \vdots & \vdots \\ m_{l,i}(\boldsymbol{A}_1) & m_{l,i}(\boldsymbol{A}_2) & m_{l,i}(\boldsymbol{A}_3) \\ \vdots & \vdots & \vdots \\ m_{l,n}(\boldsymbol{A}_1) & m_{l,n}(\boldsymbol{A}_2) & m_{l,n}(\boldsymbol{A}_3) \end{bmatrix} \qquad (41)$$

with $m_{l,i}(\boldsymbol{A}_1) + m_{l,i}(\boldsymbol{A}_2) + m_{l,i}(\boldsymbol{A}_3) = 1$.

The *Combination Matrix* $\boldsymbol{C}_i$ combines each hypothesis or set of hypotheses from two experts and builds the cut set of both. Depending on the quantifications given, some of the cut sets (here: the cut sets of "failure" and "no failure") may not be focal elements before or afterwards. To avoid mathematical effort, those columns and rows were dropped, which are related to empty cut sets or non-specified statements (non-focal elements with a 0% basic assignment). In case of two experts and three possible answers, as presented here, the matrix

$$\boldsymbol{C}_i = \begin{bmatrix} m_{1,i}(\boldsymbol{A}_1)\cdot m_{2,i}(\boldsymbol{A}_1) & 0 & m_{1,i}(\boldsymbol{A}_3)\cdot m_{2,i}(\boldsymbol{A}_1) \\ 0 & m_{1,i}(\boldsymbol{A}_2)\cdot m_{2,i}(\boldsymbol{A}_2) & m_{1,i}(\boldsymbol{A}_3)\cdot m_{2,i}(\boldsymbol{A}_2) \\ m_{1,i}(\boldsymbol{A}_1)\cdot m_{2,i}(\boldsymbol{A}_3) & m_{1,i}(\boldsymbol{A}_2)\cdot m_{2,i}(\boldsymbol{A}_3) & m_{1,i}(\boldsymbol{A}_3)\cdot m_{2,i}(\boldsymbol{A}_3) \end{bmatrix} \tag{42}$$

represents the combinations of focal elements exclusively assigned to the *i*-th event within the tree. The focal sum $\sigma(i)$ is the sum of all matrix elements $\boldsymbol{C}_i$. In this case, it is given by

$$\sigma(i) = 1 - \left(m_{1,i}(\boldsymbol{A}_1)\cdot m_{2,i}(\boldsymbol{A}_2) + m_{1,i}(\boldsymbol{A}_2)\cdot m_{2,i}(\boldsymbol{A}_1)\right), \tag{43}$$

considering the fact that "failure" ($\boldsymbol{A}_1$) and "no failure" ($\boldsymbol{A}_2$) are mutually exclusive. The combined basic assignments $m_i(\boldsymbol{A}_k)$ for a "failure", "no failure", and "uncertain" are

$$m_i(\boldsymbol{A}_1) = \frac{m_{1,i}(\boldsymbol{A}_1)\cdot m_{2,i}(\boldsymbol{A}_1) + m_{1,i}(\boldsymbol{A}_3)\cdot m_{2,i}(\boldsymbol{A}_1) + m_{1,i}(\boldsymbol{A}_1)\cdot m_{2,i}(\boldsymbol{A}_3)}{\sigma(i)}, \tag{44}$$

$$m_i(\boldsymbol{A}_2) = \frac{m_{1,i}(\boldsymbol{A}_2)\cdot m_{2,i}(\boldsymbol{A}_2) + m_{1,i}(\boldsymbol{A}_3)\cdot m_{2,i}(\boldsymbol{A}_2) + m_{1,i}(\boldsymbol{A}_2)\cdot m_{2,i}(\boldsymbol{A}_3)}{\sigma(i)}, \tag{45}$$

$$m_i(\boldsymbol{A}_3) = \frac{m_{1,i}(\boldsymbol{A}_3)\cdot m_{2,i}(\boldsymbol{A}_3)}{\sigma(i)} . \tag{46}$$

With $m_i(\boldsymbol{A}_k)$ as given above, the evidence measures for a "failure" and a "no failure" decision can be calculated by

$$bel_i(\boldsymbol{A}_1) = m_i(\boldsymbol{A}_1) \ ,$$

$$pl_i(\boldsymbol{A}_1) = m_i(\boldsymbol{A}_1) + m_i(\boldsymbol{A}_3) \ ; \tag{47}$$

$$bel_i(\boldsymbol{A}_2) = m_i(\boldsymbol{A}_2) \ ,$$

$$pl_i(\boldsymbol{A}_2) = m_i(\boldsymbol{A}_2) + m_i(\boldsymbol{A}_3) \ . \tag{48}$$

The next step of modelling applies the basic operations of *interval arithmetic* to the given event tree and assigns the evidential measures as input variables. The addition and multiplication operations are commutative, associative and sub-distributive. There is for $i \neq ii$,

$$[bel_i(\boldsymbol{A}_k), pl_i(\boldsymbol{A}_k)] + [bel_{ii}(\boldsymbol{A}_k), pl_{ii}(\boldsymbol{A}_k)]$$

$$= [bel_i(\boldsymbol{A}_k) + bel_{ii}(\boldsymbol{A}_k), pl_i(\boldsymbol{A}_k) + pl_{ii}(\boldsymbol{A}_k)] \ , \tag{49}$$

$$[bel_i(\boldsymbol{A}_k), pl_i(\boldsymbol{A}_k)] \cdot [bel_{ii}(\boldsymbol{A}_k), pl_{ii}(\boldsymbol{A}_k)]$$

$$= [\min[bel_i(\boldsymbol{A}_k)\cdot bel_{ii}(\boldsymbol{A}_k), bel_i(\boldsymbol{A}_k)\cdot pl_{ii}(\boldsymbol{A}_k),$$

$$pl_i(\boldsymbol{A}_k)\cdot bel_{ii}(\boldsymbol{A}_k), pl_i(\boldsymbol{A}_k)\cdot pl_{ii}(\boldsymbol{A}_k)],$$

$$\max[bel_i(\boldsymbol{A}_k)\cdot bel_{ii}(\boldsymbol{A}_k), bel_i(\boldsymbol{A}_k)\cdot pl_{ii}(\boldsymbol{A}_k),$$

$$pl_i(\boldsymbol{A}_k)\cdot bel_{ii}(\boldsymbol{A}_k), pl_i(\boldsymbol{A}_k)\cdot pl_{ii}(\boldsymbol{A}_k)],] \ . \tag{50}$$

Instead of subtraction, the complements of the evidence measures are applied; this yields

$$bel_i(\boldsymbol{A}_1) = 1 - pl_i(\boldsymbol{A}_2) \ , \tag{51}$$

$$pl_i(\boldsymbol{A}_1) = 1 - bel_i(\boldsymbol{A}_2) \ . \tag{52}$$

With the inputs and operations given, the evidence of a sequence r_j, see *Figure 2.*,can be calculated easily.

As described above, the basic operations of interval arithmetic are applied within the *DS*-ETA. Fortunately, the structure avoids the trouble that the sub-distributivity of subtraction operations may cause, e.g. as known from the *Fuzzy Fault Tree Analysis* (*f*-FTA), see [17].

4.3. Fault Tree Analysis

The *Fault Tree Analysis* (FTA) can model the failure of a single event or multiple failures which lead to a single system failure denoted as the *top event*, refer to Stephens & Talso [29]. However, the FTA is a top-down analysis versus the bottom-up approach for the Event Tree Analysis; i.e., the method identifies an undesirable top event and the contributing elements (down to the so-called *basic events*) that would precipitate it. The contributors are interconnected with the top event, using network paths through Boolean logic gates. The following basic steps are used to conduct a fault tree analysis:

- Define the top event of interest.
- Define the physical and analytical boundaries.
- Define the tree-top structure.
- Develop the path of failures for each branch to the logical initiating failure, represented by the basic event.

Figure 3 shows a typical fault tree with meshed basic events 1, 4, and 7.

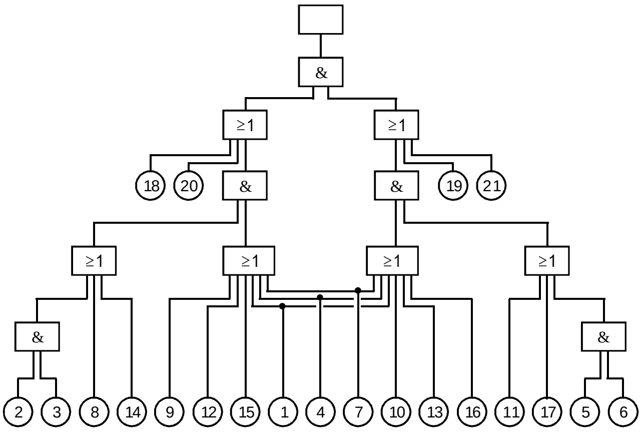

Figure 3. Typical fault tree with basic events, gates, and top event; the example represents one fault of a braking module as applied in railway vehicles

Once the fault tree has been developed to the desired degree of detail, the various paths can be evaluated to arrive at a probability of occurrence. Cut sets are combinations of components failure causing the top event. Minimal cut sets are the smallest combinations causing the top event. The method is universally applicable to systems of all kinds, with the following ground rules:

- The top events which are to be analysed, and their contributors, must be foreseen.
- Each of those top events must be analysed individually.
- The contributing factors have been adequately identified and explored in sufficient depth.

The FTA has got several strengths. The procedures are well defined and focus on failures. The top-down approach requires analysis completeness at each level before proceeding. It cannot guarantee identification of all failures, but the systematic approach enhances the likelihood of completeness. The FTA addresses effects of multiple failures by identifying interrelationships between components and identifying minimal failure combinations that cause the system to fail (minimal cut sets). The method addresses the effects of design, operation, and maintenance. The FTA can handle complex systems. It provides a graphical representation that helps to understand these complex operations and interrelationships between modules and components. Finally, FTA provides both qualitative and quantitative information.

The method is capable of producing numerical statements of the probability of occurrence of undesirable events, given probabilities of contributing factors. As Stephens & Talso ([29], page 136) claim, this capability leads to a common abuse: much effort can be expended in producing refined numerical statements of probability, based on contributing factors whose individual probabilities are hardly known and to which broad confidence limits should be attached. Applying the Dempster-Shafer Theory to FTA can help modelling uncertainties with less effort as shown by Guth [7].

Guth discusses $\Omega = \{h_1, h_2, h_3\} \equiv$ {“event occurs”, “uncertain”, “event does not occur”}. In the following, two events $\boldsymbol{A}$ and $\boldsymbol{B}$ are considered as inputs and $\boldsymbol{Z}$ as output of an And or Or gate, respectively. There is

$$m(\boldsymbol{A}_1) = bel(\boldsymbol{A})\,, \tag{53}$$

$$m(\boldsymbol{A}_2) = pl(\boldsymbol{A}) - bel(\boldsymbol{A})\,, \tag{54}$$

$$m(\boldsymbol{A}_3) = 1 - pl(\boldsymbol{A})\,, \tag{55}$$

$$m(\boldsymbol{A}_1) + m(\boldsymbol{A}_2) + m(\boldsymbol{A}_3) = 1\,; \tag{56}$$

the same holds for $\boldsymbol{B}$. Please note that the Guth approach to the *Dempster-Shafer Fault Tree Analysis* (*DS*-FTA) considers *events* where the *DS*-ETA considers *bifurcations*. *Table 8* shows the (underlying) combination of hypotheses with the different results given for the And and Or gate.

Table 8. Combination Table

And	$\boldsymbol{A}_1$	$\boldsymbol{A}_2$	$\boldsymbol{A}_3$
$\boldsymbol{B}_1$	h_1	h_2	h_3
$\boldsymbol{B}_2$	h_2	h_2	h_3
$\boldsymbol{B}_3$	h_3	h_3	h_3

Or	$\boldsymbol{A}_1$	$\boldsymbol{A}_2$	$\boldsymbol{A}_3$
$\boldsymbol{B}_1$	h_1	h_1	h_1
$\boldsymbol{B}_2$	h_1	h_2	h_2
$\boldsymbol{B}_3$	h_1	h_2	h_3

Following Step ❺ in Section 0, the combined basic assignments are calculated. An And gate yields

$$m(\boldsymbol{Z}_1) = m(\boldsymbol{A}_1)\, m(\boldsymbol{B}_1)\,, \qquad (57)$$

$$m(\boldsymbol{Z}_2) = m(\boldsymbol{A}_1)\, m(\boldsymbol{B}_2) + m(\boldsymbol{A}_2)\, m(\boldsymbol{B}_1)$$

$$+ m(\boldsymbol{A}_2)\, m(\boldsymbol{B}_2)\,, \qquad (58)$$

$$m(\boldsymbol{Z}_3) = m(\boldsymbol{A}_1)\, m(\boldsymbol{B}_3) + m(\boldsymbol{A}_2)\, m(\boldsymbol{B}_3) + m(\boldsymbol{A}_3)\, m(\boldsymbol{B}_1)$$

$$+ m(\boldsymbol{A}_3)\, m(\boldsymbol{B}_2) + m(\boldsymbol{A}_3)\, m(\boldsymbol{B}_3)$$

$$= m(\boldsymbol{A}_1)\, m(\boldsymbol{B}_3) + m(\boldsymbol{A}_2)\, m(\boldsymbol{B}_3) + m(\boldsymbol{A}_3)\,. \qquad (59)$$

For an or gate

$$m(\boldsymbol{Z}_1) = m(\boldsymbol{A}_1)\, m(\boldsymbol{B}_1) + m(\boldsymbol{A}_1)\, m(\boldsymbol{B}_2) + m(\boldsymbol{A}_1)\, m(\boldsymbol{B}_3)$$

$$+ m(\boldsymbol{A}_2)\, m(\boldsymbol{B}_1) + m(\boldsymbol{A}_3)\, m(\boldsymbol{B}_1)$$

$$= m(\boldsymbol{A}_1) + m(\boldsymbol{A}_2)\, m(\boldsymbol{B}_1) + m(\boldsymbol{A}_3)\, m(\boldsymbol{B}_1)\,, \qquad (60)$$

$$m(\boldsymbol{Z}_2) = m(\boldsymbol{A}_2)\, m(\boldsymbol{B}_2) + m(\boldsymbol{A}_2)\, m(\boldsymbol{B}_3)$$

$$+ m(\boldsymbol{A}_3)\, m(\boldsymbol{B}_2)\,, \qquad (61)$$

$$m(\boldsymbol{Z}_3) = m(\boldsymbol{A}_3)\, m(\boldsymbol{B}_3) \qquad (62)$$

holds similarly. With that, both evidence measures *bel*(***Z***) and *pl*(***Z***) can now be calculated recursively to the equations (53) to (55).

Cheng [22] claims that a calculus based on interval arithmetic is more concise and efficient in operation than the calculus proposed by Guth [7] and presented above. However, contrary to an event tree structure, a fault tree structure may cause trouble with the sub-distributivity property of subtraction operations as known from the *Fuzzy Fault Tree Analysis*, see [17]. This applies especially if events are meshed within a fault tree, see Figure 3.

Some authors apply an m: $\Omega\times\Omega \rightarrow [0, 1]$ mapping instead of the well-known m: $2^{\Omega} \rightarrow [0, 1]$ mapping which mainly characterises the calculus of the Dempster-Shafer Theory. However, an $\Omega\times\Omega$ rather represents operations in interval arithmetic, where the lower bound and the upper bound are just labelled as *belief* and *plausibility*, respectively.

4.4. Reliability Centred Maintenance

Reliability Centred Maintenance (RCM), which was first introduced in the aircraft industry, has been used with considerable success in the last decades in many industrial branches. As described in [23], the RCM analysis starts with establishing an expert group and initiating the collection of important component and system data based on the system documentation. Then the system functions are broken down to the desired component level. All relevant component information should be collected in the form of a modified FMECA. The main modification of the FMECA consists of the inclusion of information facilitating the choice of the optimum maintenance strategy. This is generally performed by an RCM decision diagram. Many different decision diagrams are proposed to apply in an RCM analysis. To illustrate the approach, a diagram as given in *Figure 4* is discussed, see [28]. Note that the given diagram is not necessarily complete or applicable in every context given.

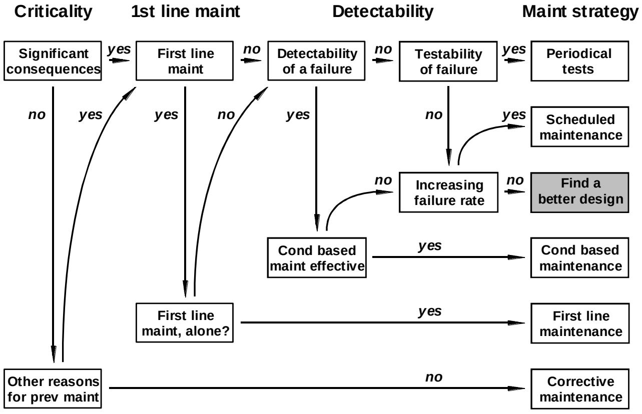

Figure 4. Example of an RCM decision diagram [23]

Supported by the diagram and the integrated questions, a choice for the best fitting maintenance strategy should be made. Finally, the maintenance program should be implemented, and feedback from operation experience and new data should be used to improve the program regularly.

The choice of the best maintenance strategy is the objective of applying RCM; however, reasoning may be difficult, due to questions without a definite answer. For example, the question whether or not a component is critical could not easily be answered with either “yes” or “no”. A Dempster-Shafer based alternative makes the avoidance of crisp “yes” or “no” decisions possible and leads to weighted recommendations on which maintenance strategy to choose.

The application of the DST to RCM (denoted as *DS*-RCM [28]) follows the procedure of the *DS*-ETA as described in Section 0. The RCM decision diagram corresponds to the event tree, where the decisions are the counterparts of the events. Consequently, the decisions “yes” and “no” correspond to the events “failure” and “no failure”. The *Expert Assessment Matrix* $\boldsymbol{M}_l$, the *Combination Matrix* $\boldsymbol{C}_i$, and the focal sum $\sigma(i)$ are defined and applied analogously. Additionally, an *RCM Decision Diagram Matrix* $\boldsymbol{D}$ with

$$\boldsymbol{D} = \begin{bmatrix} m_1(\boldsymbol{A}_1) & m_1(\boldsymbol{A}_2) & m_1(\boldsymbol{A}_3) \\ \vdots & \vdots & \vdots \\ m_8(\boldsymbol{A}_1) & m_8(\boldsymbol{A}_2) & m_8(\boldsymbol{A}_3) \end{bmatrix} \tag{63}$$

is defined, which collects the combined basic assignment values (results) of each decision within the RCM diagram. Finally, the weighted recommendations on all maintenance strategies are listed by the *Recommendation Matrix*

$$\boldsymbol{R} = \begin{bmatrix} bel(r_1) & pl(r_1) \\ \vdots & \vdots \\ bel(r_6) & pl(r_6) \end{bmatrix}, \tag{64}$$

which collects the values of the evidence measures *belief* and *plausibility* for every strategy.

The main advantages of the *DS*-RCM as against the qualitative RCM can be summarised as follows:

- Experts feel more comfortable giving degrees of belief instead of taking “yes” or “no” decisions. It might therefore be easier to obtain relevant data for the RCM analysis.
- The *DS*-RCM approach results in a profile of all possible maintenance strategies. Decision making based on this profile helps preventing “weak decisions” and may in any case be more comprehensive than relying on a single strategy.
- In some RCM studies it may be desirable to analyse modules and not separate components. In these cases *DS*-RCM is especially useful, since it does not force a single strategy.
- As shown in the discussion of the example case, the *DS*-RCM approach helps to reveal possible design problems and their causes.

A possible disadvantage of this approach is that some experts may find the evidential numbers more complicated than a simple “yes” or “no” decision. A short discussion about the nature of these numbers should therefore be given as an introduction to an RCM session.

5. Conclusions

The Dempster-Shafter Theory is well-known for its usefulness to express uncertain judgments of experts. It is shown in this contribution, how to apply the calculus to safety and reliability modelling. Approaches to expert judgement; Failure Modes, Effects, and Criticality Analysis; Event Tree Analysis; Fault Tree Analysis, and Reliability Centred Maintenance are discussed.

Generally, the Dempster-Shafter Theory adds a new flavour to safety and reliability modelling compared to probabilistic approaches. The illustration (Section 0) clearly shows the differences between the Probability and the Dempster-Shafer Theory, based on their different mappings Ω → [0, 1] versus $2^{\Omega} \rightarrow [0, 1]$, see Section 0. Probability theory would identify a single hypothesis and DST a combination of two to be responsible for the serious changes of the system considered.

6. References

6.1. Dempster-Shafer Theory

[1] Dempster, A.P. (1966). New Methods for Reasoning towards Posterior Distributions based on Sample Data. The Annals of Mathematical Statistics 37: 355-374.

[2] Dempster, A.P. (1967). Upper and Lower Probabilities Induced by a Multivalued Mapping. The Annals of Mathematical Statistics 38: 325-339.

[3] Dempster, A.P. (1968). A Generalization of Bayesian Inference. Journal of the Royal Statistical Society, Series B (methodological) 30: 205-247.

[4] Denoeux, T. (1999). Reasoning with imprecise belief structures. International Journal of Approximate Reasoning 20 (1): 79-111.

[5] Ferson, S., Kreinovich, V., Ginzburg, L., Myers, D.S. & Sentz, K. (2003). Constructing Probability Boxes and Dempster-Shafer Structures. Sandia Report SAND2002-4015.

[6] Flack, J. (1996). *On the Interpretation of Remotely Sensed Data Using Guided Techniques for Land Cover Analysis.* Unpublished PhD thesis, Department of Geographic Information Science, Curtin. University, Perth, Australia.

[7] Guth, M. A. S. (1991). A Probabilistic Foundation for Vagueness and Imprecision in Fault-Tree Analysis. *IEEE Transactions on Reliability* 40 (5), 563-571.

[8] Hollnagel, E. (1998). *Cognitive Reliability and Error Analysis Method – CREAM.* Amsterdam: Elsevier.

[9] International Electrotechnical Commission IEC, ed. (2002). International Electrotechnical Vocabulary – Chapter 191: Dependability and Quality of Service. IEC 60050-191: 2002-05, 2nd Edition.

[10] Keung-Chi, N. & Abramson, B. (1990). Uncertainty Management in Expert Systems. *IEEE Expert* 5 (2), 29-48.

[11] Klir, G. J. & Folger, T. A. (1988). *Fuzzy Sets, Uncertainty and Information. Englewood Cliffs.* Prentice-Hall.

[12] Leang, S. (1995*). A Control and Diagnostic System For The Photolithography Process Sequence*, Ph.D. Dissertation.

[13] O'Neil, A. (1999). The Dempster-Shafer Engine. http://www.quiver.freeserve.co.uk/Dse.htm

[14] Nuclear Regulatory Commission (1999). Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA), NUREG-1624.

[15] Parsons, S. (1994). Some Qualitative Approaches to Applying the Dempster-Shafer Theory. Information and Decision Technologies 19, 321-337.

[16] Rakowsky, U. K. (2005). Some Notes on Probabilities and Non-Probabilistic Reliability Measures. *Proceedings of the ESREL 2005*, Tri-City/Poland. Leiden: Balkema, 1645-1654.

[17] Rakowsky, U. K. (2002). *System Reliability* (in German), Hagen/ Germany: LiLoLe Publishing.

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

[19] Smets, P. & Kennes R. (1994). The Transferable Belief Model. *Artificial Intelligence* 66, 191-243.

[20] Walley, P. (1991). *Statistical Reasoning with Imprecise Probabilities*. London: Chapman and Hall.

[21] Yager, R. R. (1982). Generalized Probabilities of Fuzzy Events from Fuzzy Belief Structures. *Information Sciences* 28: 45-62.

6.2. Safety and Reliability Methodology

[22] Cheng, Y.-L. (2000). Uncertainties in Fault Tree Analysis. *Tamkang Journal of Science and Engineering*, Vol. 3, No. 1, 23-29.

[23] Eisinger, S. & Rakowsky, U. K. (2001). Modeling of Uncertain-ties in Reliability Centered Maintenance – A Probabilistic Approach. *Reliability Engineering and System Safety*, 71 (2), 159-164.

[24] International Electrotechnical Commission IEC (2007). *Analysis techniques for dependability – Event Tree Analysis*. IEC 62502, working document.

[25] International Electrotechnical Commission IEC (2006-a). *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*. IEC 60812:2006-01, 2nd Edition.

[26] International Electrotechnical Commission IEC (2006-b). *Fault tree analysis (FTA)*. IEC 61025:2006-12, 2nd Edition.

[27] International Electrotechnical Commission IEC (1999). *Dependability Management – Part 3-11: Application guide – Reliability centred maintenance*. IEC 60300-3-11:1999-03, 1st Edition.

[28] Rakowsky, U. K. & Gocht, U. (appears 2007). Modelling of uncertainties in Reliability Centred Maintenance – a Dempster-Shafer approach. *Proceedings of the European Conference on Safety and Reliability – ESREL 2007, Stavanger/Norway*. Approved as full paper.

[29] Stephens, R. A. & Talso, W. (1999-08). *System Safety Analysis Handbook – A Source Book for Safety Practitioners*. Unionville/Virginia, U.S.A.: System Safety Society, 2nd Edition.

7. Symbols

$\boldsymbol{A}$, $\boldsymbol{B}$	set of hypotheses
bel	belief measure
$\boldsymbol{C}$	Combination Matrix
cmn	commonality measure
$\boldsymbol{D}$	RCM Decision Diagram Matrix
h	single hypothesis
i, n	index, resp. number of an element
j	sequence index (ETA) or statement index (RCM)
k	set or statement index
l	data source index
$\boldsymbol{M}$	Expert Assessment Matrix
m	basic assignments
pl	plausibility measure
$\boldsymbol{R}$	Recommendation Matrix
r_j	sequence evidence (ETA) or evaluation value of the maintenance strategies (RCM)
$\sigma(i)$	focal sum
$\boldsymbol{Z}$	combined set of hypotheses