Towards an Improved Bowtie Method for Quantifying Industrial Risks

Thibaud de Barnier[a,b], Nelly Olivier-Maget[a], Florent Bourgeois[a], Nadine Gabas[a], Olivier Iddir[b]

[a] Laboratoire de Génie Chimique, Université de Toulouse, CNRS, INPT,UPS, 4 allée Emile Monso - CS 84234, F-31432 Toulouse cedex 4, France

[b] Technip Energies, Département Expertise & Modélisation, 2126 Boulevard de la Défense | CS 10266 | F-92741 Nanterre Cedex - France

thibaud.debarnier@technipenergies.com

Quantitative risk assessment is required by some regulations in specific situations, such as major risk evaluations. The bowtie method, which combines fault and event trees and includes safety barriers, is a valid quantitative method for analyzing industrial risks and a tool for decision-making and safety management. At present, accounting for uncertainties associated with reliability data is not necessarily mandatory in quantitative risk assessment. The quantitative method, as currently implemented, introduces uncertainties that are not addressed in the bowtie. Input data uncertainties linked to choosing values among different sources lead to variability in the results. The possibility method, presented in this article corrects this bias by considering all scenarios, without excluding those with a very low probability. For an industrial company, this specificity can allow to ensure the completeness and the robustness of its risk analysis.

This study highlights the impact of uncertainties on the quantification of a bowtie. Besides obtaining a probability, it enables decision-makers to have access to the uncertainty related to the result. This information is essential to judge the trustworthiness of the analysis and to manage risks based on uncertainties. This study allows the development of an advanced bowtie method, by considering the uncertainties associated with the input data.

1. Introduction

Bowtie (BT) risk analysis method was first introduced by the Imperial Chemical Industries Company. Following the Piper Alpha accident occurring on an oil platform in 1988, the Royal Dutch Shell Company developed this technique to improve safety of such facilities. The BT method is nowadays widely used in industry and recommended by regulatory bodies for studying major hazard scenarios (Iddir, 2015; de Rujiter and Guldenmund, 2016). It is a valuable tool for performing a detailed quantitative risk assessment, making decisions and communicating in industrial risk management (Lewis and Smith, 2010).

Figure 1 shows a representation of a BT which combines a fault tree and an event tree that are on both sides of a critical event (CE). There are several cause(C) of a CE, for example, equipment failures or human error. The fault tree describes all of the scenarios that lead to the CE. Intermediate events (IE) are defined to clarify the scenarios. The consequence scenarios depend on the success or failure of the safety barriers (SB). The quantification of the BT requires relevant input data relative to the occurrence of causes and the reliability or availability of safety barriers. Such data comes from industrial databases, feedback or from expert's judgement. In all the cases, the data include sources of uncertainties, qualified as epistemic or aleatoric, that should be considered using appropriate methods.

In the current practice, quantification of a risk consists of allocating an estimator related to its "occurrence". This estimator is a probability or a frequency that can be determined by various risk analysis methods (including the quantified bowtie). It is then compared with threshold values, which makes it possible to decide on the risk acceptability. This approach is generally implemented through a risk acceptability matrix, (a matrix that couples probability or frequency of occurrence levels and severity levels). Regardless of the chosen occurrence assessment method, the previous comparison goes through the evaluation of a point estimator (single value of

probability or frequency of occurrence). This approach facilitates decision-making since it is then relatively easy to compare it to the threshold values (the estimator being either less than or greater than the threshold value). In such processes, uncertainties are implicitly taken into account through a supposed conservatism on the input data that feeds the estimator calculation.

In recent years, risk assessment methods have improved. It is now possible to deal with the input data uncertainties and to propagate them on the output data. Moreover, functional safety standards, such as IEC 61511 (2016), recommend accounting for uncertainties in the management of safety instrumented systems in the process industry sector. Some papers, including that of Pasman and Rogers (2018), have presented various approaches of how to deal with uncertainties in a quantitative risk assessment and the follow-on decision process. They paid special attention to the highly uncertain aspect of human reliability influenced by organizational factors and conditions.
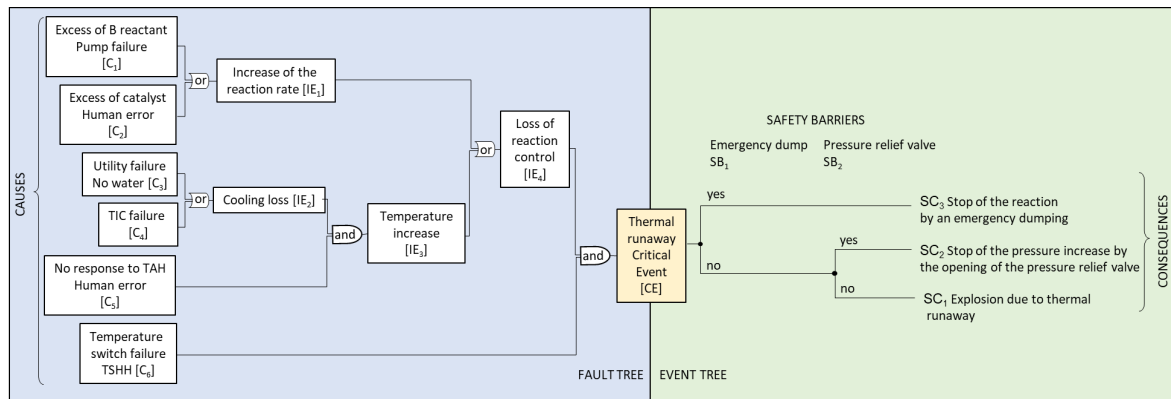

Figure 1: Bowtie of the case study

The overall objective of our work is to examine the effect of the typology of uncertainties associated with elementary bowtie events on risk assessment and associated decision-making. Section 2 is a brief overview of the types of uncertainty models encountered in risk assessment. Section 3 presents a case study used for the assessment of risk propagation under uncertainty, whose results are discussed in Section 4. The paper ends with a set of conclusion statements and perspectives.

2. Uncertainty models relevant in quantitative risk analysis

In the risk assessment framework, quantification requires assessing occurrence of causes and reliability or availability of safety barriers. The data used in quantitative risk analysis, by their very nature, are necessarily subject to uncertainty. In addition, some values are based on assumptions to fill a knowledge gap in the system. The literature distinguishes two types of uncertainties, aleatoric and epistemic (Baraldi and Zio, 2008). Aleatoric uncertainties relate to the inherent stochastic nature of the system behavior, hence the common term random uncertainty. This type of uncertainty is statistical in nature and is quantified by probability distributions. Epistemic uncertainties are uncertainties caused by a lack or incompleteness of knowledge, about failure rates in the context of risk analysis. Such uncertainty relates to the ignorance of the user about the data rather than the underlying randomness of the data. Often little is known about human errors, which is one possible occurrence of epistemic uncertainties in bowtie risk analysis. Hüllermeier and Waegeman (2021) summarise the differences between these uncertainties by saying that "epistemic uncertainty refers to the reducible part of the (total) uncertainty, whereas aleatoric uncertainty refers to the irreducible part", making the point that the stochastic component of random uncertainty is not reducible with additional knowledge. To deal with the type of knowledge about uncertainty, several uncertainty models have been developed. Figure 2 illustrates different types of uncertainty models that are deemed relevant in risk analysis, associated with a level of knowledge about failure rate data that decreases from left to right.
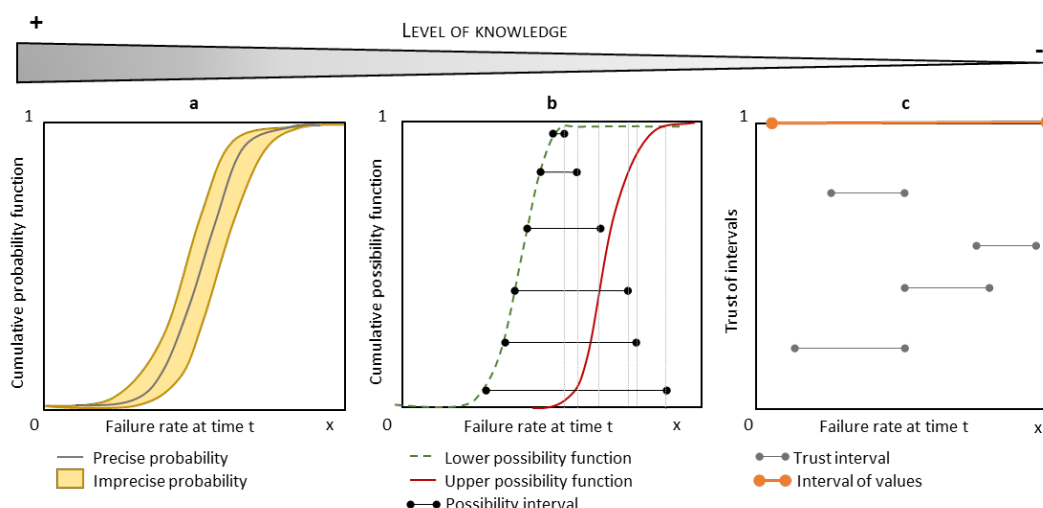
Figure 2: Uncertainty models relevant in quantitative risk analysis for aleatoric (a: precise and imprecise probabilities) and epistemic (b: possibilities; c: belief function and interval of values) uncertainties

2.1 Precise probability

Aleatoric uncertainties are quantified by precise probability distributions (Wu et al., 2020), whose propagation through the BT is carried out using Bayesian rules and Monte Carlo simulation. Such uncertainties apply typically to the failure rate of an equipment. The lognormal distribution often applies to these uncertainties, with well-documented parameters found in databases. Figure 2a shows an example of random uncertainty probability distribution.

2.2 Imprecise probability

Imprecise probabilities also apply to random uncertainties, but they carry an uncertainty about parameters of the probability distribution used to model random uncertainties (Walley, 2000; Wu et al., 2020). These parameters are themselves random variables that are quantified by a precise probability. Imprecise probabilities yield a family of distributions, as illustrated in figure 2a, that includes the precise probability as its most probable value.

2.3 Possibilities

Possibilities are one means of dealing with epistemic uncertainties. Their principles and associated calculation methods can be found in Shafer (1990) and Dubois and Prade (2015). A possibility measure can be computed from a set of nested confidence intervals (Figure 2b). The knowledge about the data is therefore divided into a finite number of intervals with given degrees of possibility called α-cuts. The greater the number of α-cuts, the more precise the results (Dubois and Prade, 2015). A confidence level is attached to each interval. A distribution of possibilities is then represented by two cumulative distributions (Figure 2b), which bracket the lower and upper limits of occurrence of the event of interest. The distance between the two distributions is a direct measure of how imprecise the data is (Baudrit et al., 2007).

2.4 Belief functions

Belief functions apply to epistemic uncertainties defined by intervals that are not nested (Shafer, 1990). It is based on the definition of belief and plausibility functions that characterise the value of the variable (Figure 2c). The number of α-cuts is limited to the number of intervals available.

2.5 Intervals

At the lower end of the knowledge scale, one may only know that a given variable lies inside a single interval (Figure 2c), defined by 2 observations. It is possible to know the minimum and maximum bounds of the probability of occurrence without being able to say anything about the distribution of this probability within this interval (Moore et al., 2009). Interval arithmetic can be used to dealing with variables defined by a single interval.

3. Case study

To illustrate the propagation of uncertainties along a bowtie, a didactic case study is considered (Figure 3). This is the semi-batch process of an exothermic reaction (A + B → C). First, reactant A is introduced at the lower part of the reactor, then reactant B is pumped into the reactor. The catalyst is added by the operator. The temperature of the reactor is controlled by a cooling system (TIC). The reactor is instrumented with a high temperature alarm (TAH), alerting the operator to stop the dosing and open the cooling valve fully. If there is no response from the operator, a safety instrumented system (TSHH) stops the dosing and opens the cooling valve fully automatically. In addition, two mitigation barriers are implemented: an emergency dump and a relief valve. The critical event studied here is thermal runaway. A corresponding simplified bowtie is shown Figure 1. It is not intended to be exhaustive about possible causes: 6 causes are considered (C_1 to C_6). Three scenarios (SC) are identified: SC_1: explosion of the reactor due to the thermal runaway, SC_2: opening of the relief valve sized on this CE, SC_3: stopping of the reaction thanks to the emergency dump. The emergency dump stops the reaction by emptying the overheating reactor into a tank containing a cold liquid.
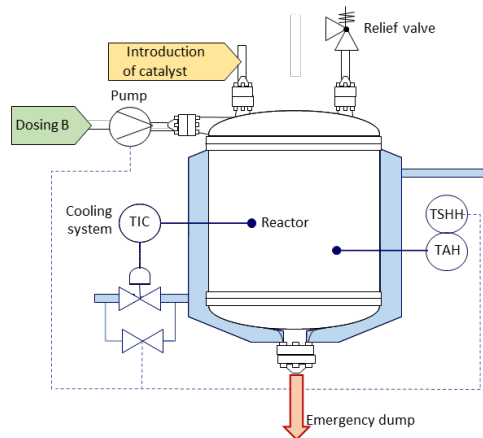

Figure 3: Schematic representation of the case study

Table 1: Reliability data of the case study

Name	Failure mode	Type of uncertainty	Uncertainty model	λ_{min}	λ_{mean} per 10^6 hr	λ_{max}
C_1	Fail to stop	aleatoric	Precise probability (lognormal distribution)	0.1	0.29	1.11
C_2	Human error to complex process	epistemic	Interval	22.83	28.53	34.24
C_3	Fail to start on demand	aleatoric	Precise probability (lognormal distribution)	0.33	2.71	7.01
C_4	TIC failure	aleatoric	Precise probability (lognormal distribution)	1.16	2.76	2.33
C_5	Human error to an unexpected event	epistemic	Interval	1.14	1.425	1.71
C_6	Process control failure	aleatoric	Precise probability (lognormal distribution)	1.16	1.88	2.76
SB_1	Fail to open on demand	aleatoric	Precise probability (lognormal distribution)	0.02	5.88	22.6
SB_2	Fail to open on demand	aleatoric	Precise probability (lognormal distribution)	0.14	4.67	15.68

Quantification of the bowtie was carried out using the data reported in Table 1. For equipment failures (C_1, C_3, C_4, C_6, SB_1 and SB_2), the data comes from the OREDA handbook (OREDA, 2015). This database contains a significant industrial dataset collected over many decades. It provides the mean failure rate λ at a reference time as well as the min and max confidence bounds at the 90% confidence level. Typically, aleatoric uncertainties with a lognormal distribution apply to equipment's failure rate. Parameters of the lognormal distribution are estimated directly from the confidence bounds of the failure rate. Human errors (C_2 and C_5) however are poorly documented, hence their uncertainties are epistemic by nature. Their rate of occurrence data is provided by experts (Villemeur, 1997). In line with section 2.5, such uncertainties should be treated as intervals. The problem was simplified by adding unsubstantiated knowledge and assuming that intervals could be modelled as precise aleatoric uncertainties using a uniform distribution. Future work will assess the effect of such an approach and the impact it has on risk assessment, considering that it is common practice.

4. Results and discussion

As explained in section 3, epistemic uncertainties present in the case study were converted to aleatoric uncertainties, so that calculation of the BT was done by propagating precise probabilities only. Calculations were performed using the commercial software GRIF® (version 2021.17) developed by Satodev, which propagates probability distributions throughout the BT by Monte-Carlo (MC) simulation. It is assumed that the barriers are not periodically tested and 100 000 draws were used for the MC simulation.

4.1 Results

Figure 4a represents the mean and 90% confidence interval of the probability of the critical event (thermal runaway) over a 2 year period. Figure 4b shows the same for the reactor explosion due to the thermal runaway (SC_1) over a 1 year period. As expected, these curves are exponentially time-dependent, which comes from the assumption that the failure probability $P(t)$ relates to the failure rate λ through $P(t)=1-e^{-\lambda t}$. Accounting for uncertainties of causes and safety barriers provides useful information, compared to the common practice of quantifying BTs using average values. For example, while the mean probability of occurrence of the critical event CE at 1 year is 0.36%, Figure 4a shows that its 90% confidence interval is [0.22%; 0.54%]. Concerning the occurrence of the reactor explosion (SC_1), the mean probability at 1 year is $6.4 \cdot 10^{-4}$ % whereas its 90% confidence interval is [$0.1 \cdot 10^{-4}$ %; $27.0 \cdot 10^{-4}$ %]. It is worth noting that the distribution of the probability of occurrence of the reactor explosion is heavily leaning towards higher probabilities. The upper bounds of these confidence intervals, which are 1.5 and 4.2 times the mean value for CE and SC1 respectively, are the values that should really matter for decision-making.
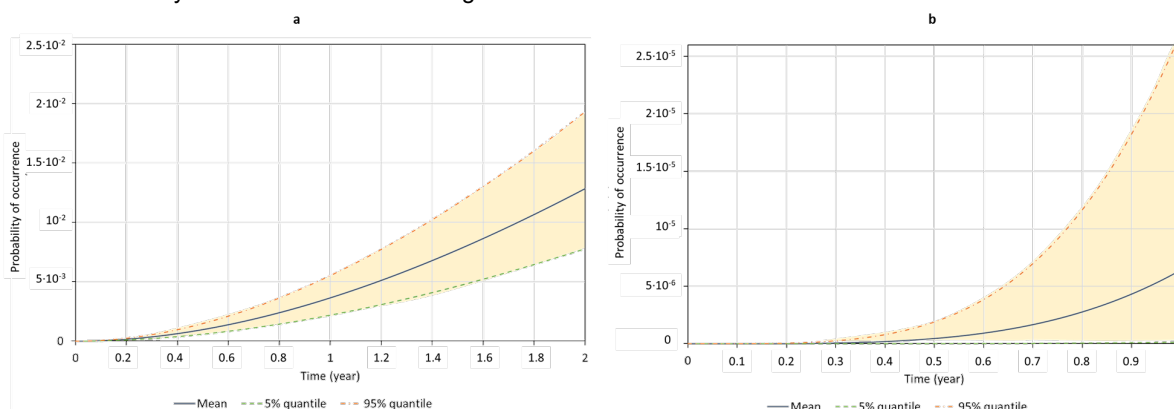

Figure 4: Probability of occurrence of the Critical Event (a: thermal runaway) and SC_1 (b: Explosion of the reactor due to thermal runaway) as a function of time

4.2 Discussion and perspectives

Overall, this short communication focussed on two important aspects of quantitative risk analysis by BT.
The first aspect concerns the taking into account of uncertainties in BTs, and more generally, in risk assessment. Let us imagine that we know that the probability of occurrence of a given critical event is in the range 1% to 5%. Should we base our decision-making on the 3% value of the mid-probability? This hardly seems justifiable. Accounting for uncertainties in risk assessment, which reflects the actual level of knowledge of the events under consideration, is the only way to obtain a true quantification of risk that can lead to informed and sound decision-making. Although not yet widely used/democratized in the field, quantification of BTs under uncertainty is rightly gaining traction, as evidenced by the development of software such as GRIF® which implements it. In concrete terms, this approach yields not a single value, but confidence bounds for the probability of occurrence of events, which may encompass several levels of risk. How to convert this information into decision-making is a topic in itself that must be addressed.
The second and complementary aspect of the problem relates to calculating BTs under uncertainty, the complexity of which is probably not unrelated to the fact that practitioners favour the use of average probability values. This paper has provided a brief inventory of how to approach uncertainties depending on the level of knowledge about the failure rate of the events considered. This led to distinguishing 2 types of uncertainties, aleatoric and epistemic, and identifying fives ways of dealing with them, namely precise probabilities, imprecise probabilities, possibilities, belief functions and intervals. While the first type of uncertainties are simple to propagate in BTs, the second type are more complex, hence the temptation to transform them abusively into the first type. This is what is exemplified in this paper by modelling epistemic uncertainties (C_2 and C_5) with a uniform distribution. This means that we have deliberately and artificially, for the sake of simplicity, increased

the level of knowledge of these two events by forcing that the probability of occurrence of human error be equiprobable everywhere inside an interval, whose existence was the only true knowledge of these events. What bias such an approach may have on risk assessment and decision-making is probably case specific. At any rate, it is not necessary to bias the actual knowledge for taking uncertainties into account in BT calculations, as hybrid methods exist that combine different uncertainty models, such a probabilities and possibilities (Baudrit et al., 2007). However, it should be borne in mind that it is in principle always possible to move from one type of uncertainty model to another for a given event, by increasing the level of knowledge of the said event, which implies the collection of additional data. Our ongoing research work is looking into all the above issues in order to produce new applicable knowledge on calculation of BTs under uncertainty for risk assessment for real industrial systems.

5. Conclusion

Quantification of risks provides quantitative and objective information about acceptability of industrial systems and possible need for additional safety barriers. Through approaches such as those presented in this paper, taking into account uncertainties in the input data associates a confidence level with the probability of occurrence of a particular event, instead of a single probability value as is the case with standard bowtie (BT) analysis.
Our research works consists precisely in propagating data along the bowtie as faithfully as is technically feasible according to the appropriate uncertainty models. Since an informed decision demands that it be associated with a confidence level, accounting for uncertainties in risk quantification is the right pathway towards industrial risk management. A point of attention along this recommended pathway is the proper handling of uncertainties, whose type, aleatoric or epistemic, is dictated by the level of knowledge for the input data used. With BTs, the question of the type and modelling of uncertainties applies to the rate of occurrence of events on both sides of the bowtie. Thus, when comparing risk reduction measures, they know whether the investment is appropriate given the uncertainties in the modelling.

References

Baraldi P., Zio E., 2008, A Combined Monte Carlo and Possibilistic Approach to Uncertainty Propagation in Event Tree Analysis, Risk Analysis, 28(5), 1309–1326.
Baudrit C., Guyonnet D., Dubois D., 2007, Joint propagation of variability and imprecision in assessing the risk of groundwater contamination, Journal of Contaminant Hydrology, 93, 72–84
Dubois D., Prade H., 2015, Practical Methods for Constructing Possibility Distributions, International Journal of Intelligent Systems, 31, 215-239.
Hüllermeier E., Waegeman W., 2021, Aleatoric and epistemic uncertainty in machine learning: an introduction to concepts and methods, Machine Learning, 110, 457–506
Iddir O., 2015, Le nœud papillon : une méthode d'analyse de risques, Environnement - Sécurité | Sécurité et gestion des risques, Les techniques de l'ingénieur, 0537.
IEC 61511, 2016, Functional Safety-Safety instrumented systems for the process industry sector (2nd ed.), International Electrotechnical Commission, Geneva.
Lewis S., Smith K., 2010, Lessons Learned from Real World Application of the Bow-tie Method. Prepared for Presentation at American Institute of Chemical Engineers - 6th Global Congress on Process Safety San Antonio.
Moore R. E., Kearfott R. B., Cloud M. J., 2009, Introduction to interval analysis, Society for Industrial and Applied Mathematics.
OREDA, 2015, Offshore and onshore REliability DAta handbook, 6th edition.
Pasman H., Rogers, W., 2018, How trustworthy are risk assessment results, and what can be done about the uncertainties they are plagued with?, Journal of Loss Prevention in the Process Industries, 55, 162–177.
de Ruijter A., Guldenmund F., 2016, The bowtie method: A review, Safety Science, 88, 211–218.
Shafer G., 1990, Perspectives on the theory and practice of belief functions, International Journal of Approximate Reasoning, 4(5–6), 323–362.
Villemeur A. ,1997, Sûreté de fonctionnement des systèmes industriels, Direction des études et recherches d'Electricité de France, Eyrolles, (1st ed).
Walley P., 2000, Towards a united theory of imprecise probability, International Journal of Approximative Reasoning, 24 (2-3), 125-148.
Wu Y., Li E., He Z.C., Lin X.Y., Jiang H.X., 2020, Robust concurrent topology optimization of structure and its composite material considering uncertainty with imprecise probability, Computer Methods in Applied Mechanics and Engineering, 364, 112927.