Computer Science and Information Systems 12(2):567–585 DOI: 10.2298/CSIS140925017V

Fuzzified Risk Management: Selection of Safeguards to Minimize the Maximum Risk

Eloy Vicente, Alfonso Mateos, and Antonio Jiménez-Martín

Decision Analysis and Statistics Group, Departamento de Inteligencia Artificial
Universidad Politécnica de Madrid, Avda. Ramiro de Maeztu 7, 28040, Madrid, Spain
{e.vicentecestero, alfonso.mateos, antonio.jimenez}@upm.es

Abstract. Threats can trigger incidents in information systems (IS) causing damage or intangible material loss to assets. A good selection of safeguards is critical for reducing risks caused by threats. This paper deals with the selection of failure transmission, preventive and palliative safeguards that minimize the maximum risk of an IS for a specified budget. We assume that all the elements in the IS are valuated using a linguistic scale, which is capable of accounting for imprecision and/or vagueness concerning the inputs. Trapezoidal fuzzy numbers are associated with these linguistic terms, and risk analysis and management is consequently based on trapezoidal fuzzy number arithmetic. We model and solve the respective fuzzy optimization problem by means of the simulated annealing metaheuristic and give an example to illustrate the safeguard selection process.

Keywords: Selection of safeguards, risk analysis, information systems, fuzzy logic.

1. Introduction

Several methodologies based on ISO/IEC 27000 [9,10,11,12] have been developed to deal with risk analysis and management in information systems (IS), such as MAGERIT by the Spanish Ministry of Public Administrations [16]; CRAMM by the Central Computing and Telecommunications Agency (UK) [3]; or NIST SP 800-30 by the National Institute of Standard and Technology (USA) [20].

These methodologies do not, however, consider imprecise ratings; they use precise values on different, usually percentage, scales. Besides, experts may find it difficult to elicit crisp values for the input parameters in risk analysis. In [27] we proposed an extension of the MAGERIT methodology for risk analysis and management based on classical fuzzy computational models. The experts could select linguistic terms from a linguistic term scale to represent these values, such as probabilities or the consequences of events. Trapezoidal fuzzy numbers were then associated with these linguistic terms and risk analysis and management computations were based on trapezoidal fuzzy number arithmetic.

The interest of the linguistic approach for risk analysis in IS is because it is located halfway between quantitative and qualitative approaches, overcoming the disadvantages of both, as advocated in [17,27,35] and discussed here.

In this paper, we review the fuzzy extension of MAGERIT methodology and focus on risk management, specifically as regards the selection of safeguards, which is crucial for dealing with threats in an IS. Preventive safeguards reduce the frequency of threats, whereas palliative safeguards reduce the degradation caused by threats to assets and fault

transmission safeguards reduce the fault transmission probability between a pair of consecutive assets.

Suppose that we have a set of threats that have to be considered sequentially to compute the risk in the IS. However, no information about this sequentiality is available. Consequently, we have a fuzzy multi-objective optimization problem whose objective functions represent new (reduced) risks as a result of the possible application of preventive and palliative safeguards regarding these threats and the application of failure transmission safeguards subject to a financial budget. As these risks are not summable, we decided to minimize the maximum risk.

The resulting optimization problem is a fuzzy combinatorial optimization problem since its complexity increases with the dimension of the asset network. Moreover, the solutions would be less computationally feasible with a larger asset network, since it would be more involved to compute the new failure transmission probabilities across the network.

Metaheuristics have to be used to solve this especially complex and combinatorial problem. Specifically, we propose using the simulated annealing (SA) metaheuristic. SA is a trajectory-based metaheuristic that considers a new solution in each iteration of the search process. The acceptance of worse solutions makes for a broader search for the optimal solution and avoids trapping in local optima in early iterations. A diversified search, in which practically all moves are allowed, is carried out in the early iterations of the search process. This becomes more and more intensive as the iterations progress until a local search is performed in the final iterations, where only better moves will be accepted.

In the next section we briefly describe the extension of the MAGERIT methodology based on classical fuzzy computational models. In Section 3 we tackle with selection of safeguards for risk management. A fuzzy optimization problem is modeled to perform this selection process, and a simulated annealing technique is proposed to solve the problem. In Section 4, we illustrate the selection of safeguards with an example. Finally, some conclusions are provided in Section 5.

2. A fuzzy extension of MAGERIT methodology

The international standards [9,10,11,12] that establish information security management systems (ISMS) certification requirements are based on BS 7799 published by BSI (British Standards Institution). The first part of the standard (BS 7799-1), published in 1995, established, for the first time, a set of best practices for information security management to be used by any company or organization, while the second part (BS 7799-2), published in 1998, established information security management system requirements for certification by independent audits.

In 1999, the ISO/IEC JTC 1 committee adopted BS 7799-1 without major changes as ISO/IEC 17799. It was renamed ISO/IEC 27002 in 2005, while the standard BS 7799-2 was adopted as ISO/IEC 27001. This is the main standard in the ISO/IEC 27000 standard series (27000 to 27019 and 27030 to 27044), which provides the framework for information security management underpinning the adoption of different IS risk analysis and management methodologies by national or corporate bodies. Specifically, the MAGERIT

methodology ([16]) was established in Spain by the Spanish Ministry of Public Administrations.

According to the MAGERIT methodology, an information system [21] consists of a set of *assets*, $\mathtt{A} = \{A_1, ..., A_n\}$. An *asset* is anything that is of value to the organization and therefore requires protection. These assets are divided into *terminal assets*, $\mathtt{A}^T = \{A_{s+1}, ..., A_{s+t}\}$, which often account for the total value of the IS and are usually data, information or business processes, and *support assets* (hardware, software, personnel, facilities...), $\mathtt{A}^S = \{A_1, ..., A_s\}$, which support terminal assets enabling data processing and proper services development. Therefore, let us suppose that the assets, $A_1, ..., A_n$, are arranged so that the first s assets are support assets and the others are terminal assets, i.e., $\mathtt{A} = \mathtt{A}^S \cup \mathtt{A}^T$ and $n = s + t$.

Although essential, support assets are a continuous source of threats and constitute the *vulnerabilities* of the IS, since a support asset failure may prevent the correct operation of terminal assets. In fact, IS assets are interrelated, forming a directed and acyclic graph. Thus, a failure in one asset can be propagated via other assets to the terminal assets, which are located at the end of the graph, causing huge losses for the organization.

Risk analysis in IS entails computing the failure transmission probabilities between the system assets, the value of the terminal assets, the degradation caused by threats and their probabilities of materialization or frequencies, and, risk management then establishes *safeguards* to prevent the materialization of the threats or reduce their impact. There are, however, no historical data, nor any possibility of putting in place mechanisms for obtaining empirical data. Consequently, subjective knowledge from experts is the only way to determine these factors.

The MAGERIT methodology offers two models: an ordinal symbolic qualitative model and a non-fuzzy quantitative model.

Qualitative model. This model establishes an ordinal scale:

$$V = \{v_0, ..., v_{n-1}\} \overset{\varphi}{\approx} [0, n-1].$$

The different magnitudes of risk are rated on this scale, where v_0 is a term under which the magnitude is considered negligible. For example, it can be said that the impact of a particular threat on an asset is $v_i \in V$. The operators considered in this qualitative model are: 1) max and min operators; and 2) product by scalars in $[0, 1]$, which can represent magnitudes such as the degradation associated with the materialization of a threat on an asset or the potential reduction of the impact of the threat thanks to a safeguard. For example, if a certain safeguard reduces impact v_i by $\alpha\%$, then this impact is reduced to a level $\beta = v_i \times (1 - \frac{\alpha}{100}) = \varphi(v_i) \times (1 - \frac{\alpha}{100}) = i \times (1 - \frac{\alpha}{100}) \in [0, n-1]$.

The result will not necessarily be a linguistic term on the given scale. In the MAGERIT methodology, a linguistic scale term is assigned to the result of these operators by rounding. This is computed in the example above as $\phi(\beta) = round(\beta) = round(i \times (1 - \frac{\alpha}{100})) \in [0, n-1] \cap \mathbb{N} = \{v_0, ..., v_{n-1}\}$.

For example, using the scale $\{v_0, ..., v_4\}$, let us asume that a threat implies an impact value v_3 on an information asset and that the frequency of the threat is 0.4. Then, MAGERIT computes the risk associated with this threat on the asset as $0.4 \times v_3 = 0.4 \times \varphi(v_3) = 0.4 \times 3 = 1.2$ and $\phi(1.2) = v_1$. So the result is a risk of v_1.

This methodology has several drawbacks:

1. It is necessary to assess some magnitudes, such as the degradation or the frequency of a threat, by means of precise percentages. Some operations, such as the product or the sum of linguistic terms, are not allowed because the results of these operations may be out of range $[0, n-1]$.
2. A lot of information is lost through the rounding. Note that the function ϕ is not bijective.
3. Such terms as $0.5 \times v_3 = 1.5$ are somewhat ambiguous. We do not know whether this value should be assigned to v_1 or v_2.
4. It needs symmetric and uniformly distributed linguistic terms scales.

Other symbolic models solve some of these drawbacks. For example, the 2-tuple model [14] is an ordinal symbolic computation model designed to solve the problem of discretizing the operation space on the linguistic term scale. The results of symbolic operations performed on the scale $\mathcal{L} = \{l_0, ..., l_{n-1}\} \approx [0, n-1]$ are given by tuple (l_i, α), where l_i is the linguistic term closest to the result and $\alpha \in [-0.5, 0.5)$ represents the distance to the term. For example, if an operation on the symbolic scale $\{l_0, ..., l_4\}$ outputs the value 3.25, then that value is the tuple $(l_3, 0.25)$

We then get the function $\Delta : [0, n-1] \longrightarrow \mathcal{L} \times [-0.5, 0.5)$ with $\beta \longmapsto \Delta(\beta) = (l_i, \alpha)$, $i = round(\beta)$ (the rounding operator) and $\alpha = \beta - i$.

It is verified that Δ is bijective, and its inverse is $\Delta^{-1}(l_i, \alpha) = i + \alpha$. This guarantees the preservation of information. However, the 2-tuple method does not allow non-linear operators. Three linear operators are introduced in [6]: the arithmetic mean, the weighted average and the OWA (ordered weighted aggregation) operator. The methods reported in [31,32] are based on the 2-tuple model and extend the number of operators that can be used, but they do not include the product of linguistic terms.

Quantitative model. This model directly measures each magnitude in the range [0,1] so that the minimum value corresponds to zero and the maximum to one. The main drawback of this model is that experts may find it difficult to assign precise values to the model input parameters, and the results are sensitive to these values.

Following [27], experts can, as an alert native to previous models, select linguistic terms from a linguistic term scale to represent these values, see Table 1 and Fig. 1. Trapezoidal fuzzy numbers are usually associated with these linguistic terms and risk analysis and management computations are based on trapezoidal fuzzy number arithmetic.

Table 1. Linguistic term scale

Term	Trapezoidal fuzzy number
Very low (VL)	(0, 0, 0, 0.25)
Low (L)	(0, 0.05, 0.15, 0.25)
Medium low (ML)	(0.15, 0.25, 0.35, 0.45)
Medium (M)	(0.35, 0.45, 0.55, 0.65)
Medium high (MH)	(0.55, 0.65, 0.75, 0.85)
High (H)	(0.75, 0.85, 0.95, 1)
Very high (VH)	(0.95, 1, 1, 1)

Fuzzy logic was introduced by Lofty A. Zadeh in 1965 [33]. A normalized trapezoidal fuzzy number with support in the interval $[a_1, a_4]$ is a t-tuple $\widetilde{A} = (a_1, a_2, a_3, a_4)$, with $a_1 \leq a_2 \leq a_3 \leq a_4$, and a function $\mu_{\widetilde{A}}(x) : \Re \longrightarrow [0, 1]$. Let us denote by $\Re^{\mathcal{TF}}$ the set of all these numbers.

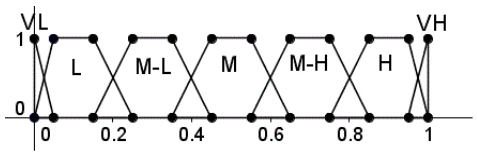

Fig. 1. Membership functions scale of fuzzy numbers

We consider the usual arithmetic for trapezoidal fuzzy numbers [30] and the internal composition law $\uplus$, which is used in the algorithm to compute the failure transmission probability between support and terminal assets, described in [21]:

$$(a_1, b_1, c_1, d_1) \uplus (a_2, b_2, c_2, d_2) = (a_1 + a_2 - a_1 a_2, b_1 + b_2 - b_1 b_2, c_1 + c_2 - c_1 c_2, d_1 + d_2 - d_1 d_2). \tag{1}$$

Indeed, $\uplus$ is an internal composition law in $\Re^{\mathcal{TF}}$, and specifically in $[0, 1]^{\mathcal{TF}}$, because if $0 \leq a_1 \leq b_1 \leq c_1 \leq d_1 \leq 1$ and $0 \leq a_2 \leq b_2 \leq c_2 \leq d_2 \leq 1$, then $0 \leq a_1 + a_2 - a_1 a_2 = 1 - (1 - a_1)(1 - a_2) \leq 1 - (1 - b_1)(1 - b_2) = b_1 + b_2 - b_1 b_2 \leq 1$. Analogously, $0 \leq b_1 + b_2 - b_1 b_2 \leq c_1 + c_2 - c_1 c_2 \leq d_1 + d_2 - d_1 d_2 \leq 1$.

Following the risk analysis methodology, first, the failure transmission probability $\widetilde{D}(A_i, A_k)$ is computed considering all possible paths connecting A_i with A_k, as well as the failure transmission probability between two consecutive assets A_u and A_v belonging to a path from A_i to A_k in the graph, $\widetilde{d}(A_u, A_v)$. For example, the failure transmission probability from A_1 to A_4 in Fig. 2(a) is computed as

$$\begin{aligned} \widetilde{D}(A_1, A_4) &= \widetilde{d}(A_1, A_3) \otimes \widetilde{d}(A_3, A_4) \uplus \widetilde{d}(A_1, A_2) \otimes \widetilde{d}(A_2, A_4) = \\ &= \widetilde{d}(A_1, A_3) \otimes \widetilde{d}(A_3, A_4) \oplus \widetilde{d}(A_1, A_2) \otimes \widetilde{d}(A_2, A_4) \ominus \\ &\ominus \widetilde{d}(A_1, A_3) \otimes \widetilde{d}(A_3, A_4) \otimes \widetilde{d}(A_1, A_2) \otimes \widetilde{d}(A_2, A_4). \end{aligned}$$

The algorithm proposed in [21] can be used for computing failure transmission probabilities in more complex ISs. The failure transmission probability from A_i to A_k, $\widetilde{D}(A_i, A_k)$, is computed as follows. We denote by **P**=$\{P_1, ..., P_s\}$ the set of paths in the analysis of the failure transmission from A_i to A_k. Then,

A) If all assets (excluding A_i and A_k) in the paths in **P** are influenced by only one asset, then

$$\widetilde{D}(A_i, A_k) = \overset{s}{\underset{j=1}{\oplus}} \widetilde{D}(A_i, A_k | P_j), \tag{2}$$

where $\widetilde{D}(A_i, A_k | P_j) = \widetilde{d}(A_i, A_{j1}) \otimes \widetilde{d}(A_{j1}, A_{j2}) \otimes ... \otimes \widetilde{d}(A_{jn}, A_k)$, and $P_j : (A_i \rightarrow A_{j1} \rightarrow A_{j2} \rightarrow ... \rightarrow A_{jn} \rightarrow A_k)$.

B) Otherwise, we assume that the first r paths in **P** are formed by assets (excluding A_i and A_k) influenced by only one asset, and the remaining $s-r$ paths include at least one asset influenced by two or more assets. Then, for the r first paths, we proceed as in A), and we denote by **S** the set including the $s-r$ remaining paths. We proceed with **S** as follows:

(i) Compute the set of non-terminal assets in **S** influenced by two or more assets, denoted by I, and the subset of I including assets uninfluenced by any other asset in I, denoted by NI.

(ii) Consider an asset A_r in NI and then simplify the paths in **S** that include asset A_r making $A_i \rightarrow A_r \rightarrow ... \rightarrow A_k$, with $\widetilde{d}(A_i, A_r) = \widetilde{D}(A_i, A_r)$ (computed as in *A)*).

(iii) Remove repeated paths from **S** and keep only one instance.

(iv) Build I and NI again from **S**.

(v) If NI is not empty, go to (ii). Otherwise, the algorithm finishes.

Let us denote the resulting set of paths by **S=** $\{P'_1, ..., P'_m\}$, with $m \leq s-r$. Then, the degree of dependency of A_k regarding A_i is

$$\widetilde{D}(A_i, A_k) = \overset{r}{\underset{j=1}{\oplus}} \widetilde{D}(A_i, A_k|P_j) \overset{m}{\underset{l=1}{\oplus}} \widetilde{D}(A_i, A_k|P'_l). \tag{3}$$

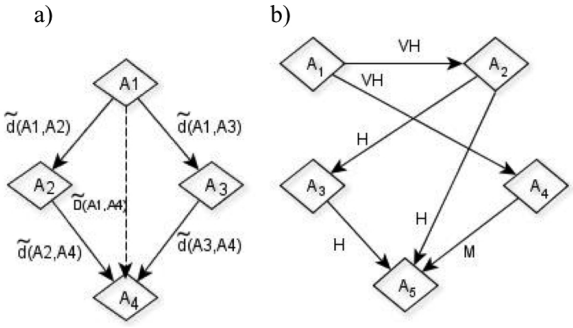

Fig. 2. Examples of ISs.

Assets are usually evaluated by taking into account three components: *confidentiality*, *integrity* and *authenticity*. A very common practice is to give each component a monetary value, i.e., attempt to quantify the losses that would be incurred if there were a breach of the confidentiality of terminal assets, the terminal assets were damaged or the terminal assets were unavailable for any length of time. This is a practice recommended by international standards based on ISO 27000 [3,9,12,16,20]. Let us denote the value of the terminal asset A_k by $\widetilde{\mathbf{v}}_k = (\widetilde{v}_{k1}, \widetilde{v}_{k2}, \widetilde{v}_{k3})$.

When a *threat* to a support asset A_i materializes, causing a failure, the organization's biggest concern is to prevent the failure from being transmitted to terminal assets, since this would lead to losses in the value components. We denote by T_j^i the j-th threat to asset A_i, $i = 1, ..., n$, $j = 1, ..., n_i$. T_j^i is defined by the corresponding *degradation* of value

components, $\widetilde{\mathbf{d}}^{T_j^i} = (\widetilde{d}_1^{T_j^i}, \widetilde{d}_2^{T_j^i}, \widetilde{d}_3^{T_j^i})$, and the frequency $\widetilde{f}^{T_j^i}$ with which the threat to A_i materializes, where $\widetilde{d}_l^{T_j^i}$ and $\widetilde{f}^{T_j^i}$ are represented by a linguistic term and the respective trapezoidal fuzzy number. Then, the *impact* that threat T_j^i has on the terminal asset A_k, with degradation $\widetilde{\mathbf{d}}^{T_j^i}$, is $\widetilde{\mathbf{I}}_k^{T_j^i} = (\widetilde{d}_1^{T_j^i} \times \widetilde{v}_{k1}, \widetilde{d}_2^{T_j^i} \times \widetilde{v}_{k2}, \widetilde{d}_3^{T_j^i} \times \widetilde{v}_{k3})$.

Finally, the *risk* to asset A_k caused by the threat T_j^i is the product of the impact on the terminal asset multiplied by the probability, $\widetilde{p}$, of this threat reaching asset A_k: $\widetilde{\mathbf{R}}_k^{T_j^i} = \widetilde{p} \times \widetilde{\mathbf{I}}_k^{T_j^i} = \widetilde{p} \times \left(\widetilde{d}_1^{T_j^i} \otimes \widetilde{v}_{k1}, \widetilde{d}_2^{T_j^i} \otimes \widetilde{v}_{k2}, \widetilde{d}_3^{T_j^i} \otimes \widetilde{v}_{k3} \right)$.

However, $\widetilde{p}$ is the product of the frequency $\widetilde{f}^{T_j^i}$ multiplied by the failure transmission probability between assets A_i and A_k, $\widetilde{D}(A_i, A_k)$. Therefore,

$$\widetilde{\mathbf{R}}_k^{T_j^i} = \left(\widetilde{R}_{k1}^{T_j^i}, \widetilde{R}_{k2}^{T_j^i}, \widetilde{R}_{k3}^{T_j^i} \right) = \widetilde{D}(A_i, A_k) \otimes \widetilde{f}^{T_j^i} \otimes \widetilde{\mathbf{I}}_k^{T_j^i} =$$
$$= \widetilde{D}(A_i, A_k) \otimes \widetilde{f}^{T_j^i} \otimes \left(\widetilde{d}_1^{T_j^i} \otimes \widetilde{v}_{k1}, \widetilde{d}_2^{T_j^i} \otimes \widetilde{v}_{k2}, \widetilde{d}_3^{T_j^i} \otimes \widetilde{v}_{k3} \right).$$

The *total risk* for each component l ($l = 1, 2, 3$) of the IS for threat T_j^i is the sum of the risk for each terminal asset:

$$\widetilde{R}_l^{T_j^i} = \bigoplus_{k=m+1}^{n} \left(\widetilde{D}(A_i, A_k) \otimes \widetilde{f}^{T_j^i} \otimes \widetilde{v}_{kl} \otimes \widetilde{d}_l^{T_j^i} \right). \tag{4}$$

Note that a similarity function is required to associate the resulting trapezoidal fuzzy number with an element in the linguistic term set. This function can also be used at any step of the methodology to derive the linguistic terms associated with the respective trapezoidal fuzzy numbers output to represent dependencies, accumulated values, etc.

For instance, we could use the similarity function proposed in [23,24], which accounts for the shared area between the generalized fuzzy numbers with respect to the total area of these fuzzy numbers in addition to the geometric distance and the distance between the centers of gravity: Given two trapezoidal fuzzy numbers $\widetilde{A} = (a_1, a_2, a_3, a_4)$ and $\widetilde{B} = (b_1, b_2, b_3, b_4)$, their similarity can be computed by

- if $\max\{(a_4 - a_1), (b_4 - b_1)\} \neq 0$ (non-empty intersection), then
  $S(\widetilde{A}, \widetilde{B}) = 1 - (1 - \alpha - \beta) \left(1 - \frac{\int_0^1 \mu_{\widetilde{A} \cap \widetilde{B}}(x) dx}{\int_0^1 \mu_{\widetilde{A} \cup \widetilde{B}}(x) dx} \right) - \alpha \frac{\sum |a_i - b_i|}{4} - \beta d \left[(x_{\widetilde{A}}, y_{\widetilde{A}}), (x_{\widetilde{B}}, y_{\widetilde{B}}) \right],$
- otherwise,
  $S(\widetilde{A}, \widetilde{B}) = 1 - \left(\frac{1 - \alpha - \beta}{2} + \alpha \right) \cdot \frac{\sum |a_i - b_i|}{4} - \left(\frac{1 - \alpha - \beta}{2} + \beta \right) \cdot d \left[(x_{\widetilde{A}}, y_{\widetilde{A}}), (x_{\widetilde{B}}, y_{\widetilde{B}}) \right],$

where $\alpha + \beta < 1$, $\mu_{\widetilde{\chi}}$ is the membership function of $\widetilde{\chi}$, $\mu_{\widetilde{A} \cap \widetilde{B}}(x) = \min\limits_{0 \leq x \leq 1} \{\mu_{\widetilde{A}}(x), \mu_{\widetilde{B}}(x)\}$, $\mu_{\widetilde{A} \cup \widetilde{B}}(x) = \max\limits_{0 \leq x \leq 1} \{\mu_{\widetilde{A}}(x), \mu_{\widetilde{B}}(x)\}$, $(x_{\widetilde{A}}, y_{\widetilde{A}}), (x_{\widetilde{B}}, y_{\widetilde{B}})$ are the centers of gravity of $\widetilde{A}$ and $\widetilde{B}$, and d is a distance in $\mathbb{R}^2$.

Note that direct assignments based on a rigid linguistic term scale is not always advisable since the expert has no say in the number of linguistic terms that the scale is to include and about the appearance of their associated trapezoidal fuzzy numbers. Instead

we propose the use of the betting and lottery-based method for fuzzy probability elicitation described in [27].

Betting and lottery-based methods are commonly used to assign probabilities and can also be used to assign fuzzy probabilities ([19,7]). In *betting methods*, given two selected monetary values $x > y$, the expert chooses one of the following two gambles:

- *b1*: If event A happens, then you win $x\$$. Otherwise, you lose $y\$$.
- *b2*: If event A does not happen, then you win $y\$$. Otherwise, you lose $x\$$.

An interactive process is enacted until two alternative gambles to which the expert is indifferent are reached, and it follows that $p(A) = x/(x+y)$. In this process, if the expert is not indifferent, then the expected utility of the selected gamble should be higher than for the rejected gamble. Then, the analyst has to update monetary values and offer the expert two new gambles.

In *lottery-based methods*, given a probability and monetary values $x\$$ and $y\$$, the expert chooses between the following lotteries:

- *l1*: If event A happens, then you win $x\$$. Otherwise, you lose $y\$$.
- *l2*: You win $x\$$ with probability p, or $y\$$ with probability $1 - p$.

An interactive process is again enacted, in which the value p has to be readjusted until two lotteries to which the expert is indifferent are reached.

A realistic scenario is where experts have an interval rather than a precise value in mind at the point when they are indifferent to either bet or lottery, that is, for the lottery-based method there will be an interval $[a, c]$ such that if $p = [a, c]$, then the expert has no preference for either lottery $l1$ or $l2$. Similarly, the betting method can result in an interval of indifference $[b, d]$.

On the other hand, it is recommendable to use several methods to test for expert consistency and bias. In this regard, the following algorithm can be used to derive a fuzzy probability on the basis of betting and lottery-based methods ([27]):

- If $[a, c] \cap [b, d] = \emptyset$, then the expert's probabilistic judgment is inconsistent.
- If any of the intervals is contained in the other $[a, c] \subseteq [b, d]$ (or $[b, d] \subseteq [a, c]$), then we assume that the trapezoidal fuzzy number (b, a, c, d) (or (a, b, d, c)) designates the expert's probabilistic judgment.
- If $[a, c] \cap [b, d] \neq \emptyset$, is uncountable, and none of the intervals is contained in the other, then, assuming that $a \leq b \leq c \leq d$, (a, b, c, d) designates the expert probabilistic judgment.

This is a more efficient way of allocating the probability of an event without the biases inherent in the use of linguistic scales. Nevertheless, direct assignment based on linguistic scales is much faster and more usual in decision-making processes involving fuzzy logic.

3. Optimal selection of safeguards in risk management

The safeguards that should be implemented to reduce the total risk in the IS have to be identified according to the established risk indicators for each threat to the IS.

Safeguards can be *preventive*, if they reduce the frequency $\widetilde{f}$ of threats; *palliative*, if they reduce the degradation $\widetilde{\mathbf{d}}$ caused by threats to assets; or *fault transmission safeguards*, if they reduce the fault transmission probability between a pair of consecutive assets, i.e., $\widetilde{d}(A_u, A_v)$.

Let us denote the sets of safeguards by:

- $S : \{S_t^{uv}, u, v = 1, ..., n; t = 1, ..., n_{uv}\}$ is the set of failure transmission safeguards, where S_t^{uv} is the t-th failure transmission safeguard between the consecutive (connected) assets A_u and A_v. The corresponding effect of each safeguard S_t^{uv} on the failure transmission probability $\widetilde{d}(A_u, A_v)$ is denoted by $\widetilde{e}^{S_t^{uv}}$ and its cost by c_t^{uv}.
- $S^{(pr)} : \{S_t^{(pr)T_j^i}, i = 1, ..., n; j = 1, ..., n_i; t = 1, ..., m_{ij}^{pr}\}$ is the set of preventive safeguards, where $S_t^{(pr)T_j^i}$ is the t-th preventive safeguard for the j-th threat to asset A_i. Its effect on the frequency of the threat T_j^i is $\widetilde{e}^{S_t^{(pr)T_j^i}}$ and its cost is $c_t^{(pr)T_j^i}$.
- $S^{(pa)} : \{S_t^{(pa)T_j^i}, i = 1, ..., n; j = 1, ..., n_i; t = 1, ..., m_{ij}^{pa}\}$ is the set of palliative safeguards, where $S_t^{(pa)T_j^i}$ is the t-th palliative safeguard for the j-th threat to asset A_i. Its effect on the degradation in the component l of the threat T_j^i is $\widetilde{e}_l^{S_t^{(pa)T_j^i}}$ and its cost is $c_t^{(pa)T_j^i}$.

We can select different packages of safeguards to reduce risk. These packages will be represented by binary vectors $\mathbf{x}_{uv} = (x_t^{uv})_{t=1}^{n_{uv}}$, $\mathbf{x}_{ij}^{pr} = (x_t^{(pr)T_j^i})_{t=1}^{m_{ij}^{pr}}$, $\mathbf{x}_{ij}^{pa} = (x_t^{(pa)T_j^i})_{t=1}^{m_{ij}^{pa}}$, respectively, where $x_t^{uv} = 1$, $x_t^{(pr)T_j^i} = 1$ and $x_t^{(pa)T_j^i} = 1$ if the t-th safeguard S_t^{uv}, $S_t^{(pr)T_j^i}$ and $S_t^{(pa)T_j^i}$ is selected, respectively. Besides, we denote by $\mathbf{c}_{uv} = (c_1^{uv}, ..., c_{n_{uv}}^{uv})$, $\mathbf{c}_{ij}^{pr} = (c_1^{(pr)T_j^i}, ..., c_{m_{ij}^{pr}}^{(pr)T_j^i})$ and $\mathbf{c}_{ij}^{pa} = (c_1^{(pa)T_j^i}, ..., c_{m_{ij}^{pa}}^{(pa)T_j^i})$ the safeguard cost vectors.

If the effect of a safeguard is $e\%$ or in *per one*, then its parameter is reduced by that amount. The effect caused by a safeguard can be also represented by a linguistic term from the scale in Table 1. For example, the probability of a threat after the implementation of a preventive safeguard with effect $\widetilde{e}$ is reduced to the level $(\widetilde{1} \ominus \widetilde{e}) \otimes \widetilde{f}$.

Note that $\ominus$ is not an internal composition law in TF[0,1]. However,

- $\widetilde{A}, \widetilde{B} \in TF[0,1] \Rightarrow \widetilde{A} \otimes (\widetilde{1} \ominus \widetilde{B}) \in TF[0,1]$,
- $\widetilde{A} \otimes (\widetilde{1} \ominus \widetilde{B}) \leq \widetilde{A}$ with the partial order of the trapezoidal fuzzy numbers (i.e., $\widetilde{A} \leq \widetilde{B} \Leftrightarrow a_1 \leq b_1, a_2 \leq b_2, a_3 \leq b_3, a_4 \leq b_4$) and
- $\widetilde{A} \otimes (\widetilde{1} \ominus \widetilde{B})$ decreases with $\widetilde{B}$.

In [25] we propose a method for reducing the degrees of dependency from all support assets to terminal assets minimizing the costs for the company.

As mentioned above, the probability of transmission of failure from support assets $\widetilde{D}(A_i, A_k)$ is the result of fuzzy operations with the probabilities of transmission of failure through intermediate assets linking the attacked support asset with other assets.

In each of these intermediate assets, safeguards can be enforced to reduce the probability of transmission of a failure. The effect induced by a safeguard to reduce the probability of transmission of failures between two assets A_u and A_v can also be defined as a

linguistic term, which is represented by a fuzzy number $\widetilde{e}^{u,v} \in TF[0,1]$. So, if the degree of direct dependency between assets A_u and A_v is $\widetilde{d}(A_u, A_v)$, then, when we implement a safeguard with effect $\widetilde{e}^{u,v}$, the degree of direct dependency is reduced to

$$\widetilde{d}(A_u, A_v) \otimes (\widetilde{1} \ominus \widetilde{e}^{u,v}).$$

The problem of keeping at an acceptable (low or very low) level the failure transmission probabilities among support and terminal assets with minimal costs can be represented as follows:

$$\begin{aligned} & min \sum_{u=1}^{n} \sum_{v \in N_u} \sum_{t}^{n_{uv}} c_t^{uv} x_t^{uv} \\ & \text{s. t. } \widetilde{D(A_i, A_k)} \leq \widetilde{U}_{ik} \; \forall i \in \mathtt{A}^T, k \in \mathtt{A}^S \\ & \quad x_t^{u,v} \in \{0,1\} \, \forall u, v \in N_u, t \in \{1, ..., n_{uv}\} \end{aligned} \tag{5}$$

where N_u is the set of assets connected by an arc from A_u, $\widetilde{U}_{ik}$ is a residual value accepted by the experts, $x_t^{u,v}$ are the decision variables ($x_t^{u,v} = 1$ means that safeguard $S_t^{u,v}$ is selected), and $\widetilde{D(A_i, A_k)}$ is reassessed replacing values $\widetilde{d(A_u, A_v)}$ by the affected values regarding the selected safeguards:

$$\widetilde{d(A_u, A_v)} \otimes \left[\oplus_t (\widetilde{1} \ominus \widetilde{e}_t^{u,v}) \right],$$

where A_u and A_v are two consecutive assets connected by an arc in some path between A_i and A_k.

This problem can be solved by dynamic programming and metaheuristics techniques as shown in [25]. Remember that indirect failure transmission probabilities are recursively computed following the algorithm described in Section 2. Thus, the failure transmission probabilities of the support assets further away from the terminals can be computed from the failure transmission probabilities of the closest assets. Therefore, the problem can be solved stepwise, and the principle of optimality in dynamic programming holds: Given an optimal sequence of decisions, every subsequence is, in turn, optimal. Then we proceed as follows:

- Step 0. Let $\mathtt{A}^T$ be the set of terminal assets.
- Step 1. Consider $\mathtt{A}_1^T$ including support assets whose children belong to $\mathtt{A}_0^T$ only. Identify safeguards that minimize costs keeping the failure transmission probabilities over their children at an acceptable level.
- Step 2. Consider $\mathtt{A}_2^T$ including support assets whose children belong to $\mathtt{A}_0^T \cup \mathtt{A}_1^T$ only. Identify safeguards that minimize costs keeping the failure transmission probabilities over $\mathtt{A}_0^T$ under an acceptable level. Note that the failure transmission probabilities of indirect dependency from the children of $\mathtt{A}_2^T$ to terminal assets have already been computed in the previous step, so we only need to identify the failure transmission probabilities over assets in $\mathtt{A}_0^T \cup \mathtt{A}_1^T$.
  ...
- Step *i*. Consider $\mathtt{A}_i^T$ including support assets whose children belong to $\mathtt{A}_0^T \cup \mathtt{A}_1^T \cup ... \cup \mathtt{A}_{i-1}^T$ only. Identify safeguards that minimize costs keeping the failure transmission

probabilities over $\mathbb{A}_0^T$ under an acceptable level. Note that again we only need to identify the direct failure transmission probabilities over assets in $\mathbb{A}_0^T \cup \mathbb{A}_1^T \cup ... \cup \mathbb{A}_{i-1}^T$.
...

However, we propose in this paper to reduce the risk index on terminal assets subject to a financial budget.

The optimization problem to be solved consists of minimizing the maximum risk for the IS subject to a financial budget c:

$$\begin{aligned} &min\ z = max_{i,j,l}\{\widetilde{R}_l^{T^i_j}\} \\ &\text{s. t. } \textstyle\sum_{u=1}^{n}\sum_{v\in N_u}\mathbf{c}_{uv}\cdot\mathbf{x}_{uv} + \sum_{i=1}^{n}\sum_{j=1}^{n_i}\mathbf{c}_{ij}^{pr}\cdot\mathbf{x}_{ij}^{pr} + \sum_{i=1}^{n}\sum_{j=1}^{n_i}\mathbf{c}_{ij}^{pa}\cdot\mathbf{x}_{ij}^{pa} \leq c, \end{aligned} \tag{6}$$

where $\mathbf{c}_{ik}$, $\mathbf{c}_{ij}^{pr}$ and $\mathbf{c}_{ij}^{pa}$ are safeguard cost vectors.

Note that we have a set of threats that have to be considered sequentially rather than simultaneously to compute the risk in the IS. However, no information about this sequentiality is available. Consequently, we have a fuzzy multi-objective optimization problem whose objective functions represent new (reduced) risks as a result of the possible application of preventive and palliative safeguards regarding these threats and the application of failure transmission safeguards. Thus, these risks are not summable, and we have decided to minimize the maximum risk.

The objective function has to be total order and fuzzy numbers are not. The definition of indexes to rank fuzzy trapezoidal numbers has been a transcendental issue in the history of fuzzy logic. More than thirty ranking methods for trapezoidal fuzzy numbers are described in [1,2,29]. In this paper we use the index proposed by Murakami et al [18], which computes the centroid of the compared fuzzy numbers: If $\widetilde{A} = (a_1, a_2, a_3, a_4)$ then its centre of gravity is the point $(\bar{X}_{\widetilde{A}}, \bar{Y}_{\widetilde{A}})$, with

$$\bar{Y}_{\widetilde{A}} = \frac{\frac{a_3-a_2}{a_4-a_1}+2}{6} \quad \text{and} \quad \bar{X}_{\widetilde{A}} = \bar{Y}_{\widetilde{A}}(a_3-a_2) + \left(1-\bar{Y}_{\widetilde{A}}\right)(a_4-a_1).$$

The Murakami index first compares the abscissas of the centroids. The fuzzy numbers whose centroids have bigger abscissas are better ranked. If abscissas are equal, then the one with the higher ordinate is ranked first.

The fuzzy optimization problem is a combinatorial problem: its complexity increases with the dimension of the asset network since different packages of failure transmission safeguards could be considered in each arc, and the selected safeguards for the assets closest to the terminal assets also reduce the fault transmission probability of the assets that are farthest away. Moreover, the solutions would be less computationally feasible with a larger asset network, since it would be more involved to compute the new failure transmission probabilities across the network.

Metaheuristics have to be used to solve this especially complex and combinatorial problem ($2^{\sum_{u,v} n_{ik} + \sum_{i,j} m_{ij}^{pr} + \sum_{i,j} m_{ij}^{pa}}$ possible solutions and $3 \times s$ (number of threats under consideration) fuzzy risk elements in the objective function).

Simulated annealing (SA) is one of the most used metaheuristics because of its ease of implementation and efficiency [4,15]. Its pseudocode (for a minimization problem) is as follows:

- Randomly generate an initial feasible solution x_0. Do $x^* = x_0, f^* = f(x_0), i = 0$. Select the initial temperature $T_0 = T$ (T_i temperature at step *i*).
- Repeat until the stopping criterion is satisfied:
  - Randomly generate $y \in N(x_i)$ (where $N(x_i)$ is a neighborhood of x_i)
  - If $f(y) - f(x_i) \leq 0$, then
    - $x_{i+1} = y$
    - If $(f(x^*) > f(x_i))$, then $x^* = x_i, f^* = f(x_i)$

    otherwise:
    - $p \sim U(0,1)$ (p is randomly generated in $[0,1]$)
    - If $p \leq e^{-(f(y)-f(x_i))/T_i}$, then $x_{i+1} = y$
  - Update temperature, $i = i + 1$

The basic idea of SA is as follows. An initial feasible solution is randomly generated. A new solution, y, is randomly generated from the neighborhood of the current solution at each iteration, $N(x_i)$. If the new solution is better than the current one, then the algorithm moves to that solution. Otherwise, there is a certain probability of moving to a worse solution, $e^{-(f(y)-f(x_i))/T_i}$. The acceptance of worse solutions makes for a broader search for the optimal solution and avoids trapping in local optima in early iterations. The probability of accepting a worse move is a function of both a temperature factor (T) and the change in the cost function $(f(y) - f(x_i))$. The initial value of T is high, which leads to a diversified search, since practically all moves are allowed. As T decreases, the probability of accepting a worse move falls, and only better moves will be accepted when it is zero.

4. An illustrative example

Let us consider the IS in Fig. 2(b). The asset A_5 is terminal and its monetary value (in thousands of units) is $\widetilde{\boldsymbol{v_5}} = ((10,15,20,25),(18,20,23,30),(12,15,26,30))$, for the three components, respectively.

The probabilities of failure transmission from each support asset to the terminal asset are:

$$\begin{aligned}
&\widetilde{D}(A_4,A_5) = \widetilde{d}(A_4,A_5) = M = (0.35,0.45,0.65,0.75),\\
&\widetilde{D}(A_3,A_5) = \widetilde{d}(A_3,A_5) = H = (0.75,0.85,0.95,1),\\
&\widetilde{D}(A_2,A_5) = \widetilde{d}(A_2,A_5) \uplus (\widetilde{d}(A_2,A_3) \otimes \widetilde{D}(A_3,A_5)) =\\
&\qquad = H \uplus (H \otimes H) = (0.93,0.97,0.99,1),\\
&\widetilde{D}(A_1,A_5) = (\widetilde{d}(A_1,A_4) \otimes \widetilde{D}(A_4,A_5)) \uplus \left(\widetilde{d}(A_1,A_2) \otimes \widetilde{D}(A_2,A_5)\right) =\\
&\qquad = (VH \otimes M) \uplus (VH \otimes (0.93,0.97,0.99,1)) = (0.92,0.98,0.99,1).
\end{aligned}$$

We consider five threats with frequencies and degradations shown in Table 2. The risks induced for each individual threat on the terminal asset A_5 before applying the safeguard are shown in Table 3.

Let us consider the 32 failure transmission safeguards in Table 4 and the 22 palliative and 16 preventive safeguards for the threats in Table 5. The budget is $c = 5000$ monetary

units. Then, we have to solve the following fuzzy optimization problem to identify the safeguards to be implemented:

$$min\ z = max_l\{\widetilde{R}_l^{T_1^1}, \widetilde{R}_l^{T_1^2}, \widetilde{R}_l^{T_2^2}, \widetilde{R}_l^{T_1^3}, \widetilde{R}_l^{T_1^4}\}$$

$$\text{s. t. } \sum_{u=1}^{n}\sum_{v\in V_u}\mathbf{c}_{uv}\cdot\mathbf{x}_{uv} + \sum_{i=1}^{n}\sum_{j=1}^{n_i}\mathbf{c}_{ij}^{pr}\cdot\mathbf{x}_{ij}^{pr} + \sum_{i=1}^{n}\sum_{j=1}^{n_i}\mathbf{c}_{ij}^{pa}\cdot\mathbf{x}_{ij}^{pa} \leq 5000 \tag{7}$$

with

$$\widetilde{R}_l^{T_1^1} = \widetilde{D'}(A_1, A_5)\otimes\widetilde{f}^{T_1^1}\otimes(\otimes_{t=1}^{4}(\widetilde{1}\ominus\widetilde{e}^{S_t^{(pr)T_1^1}}))\otimes\widetilde{d}_l^{T_1^1}\otimes(\otimes_{t=1}^{6}(\widetilde{1}\ominus\widetilde{e}^{S_t^{(pa)T_1^1}})),$$
$$\widetilde{R}_l^{T_1^2} = \widetilde{D'}(A_2, A_5)\otimes\widetilde{f}^{T_1^2}\otimes(\otimes_{t=1}^{2}(\widetilde{1}\ominus\widetilde{e}^{S_t^{(pr)T_1^2}}))\otimes\widetilde{d}_l^{T_1^2}\otimes(\otimes_{t=1}^{3}(\widetilde{1}\ominus\widetilde{e}^{S_t^{(pa)T_1^2}})),$$
$$\widetilde{R}_l^{T_2^2} = \widetilde{D'}(A_2, A_5)\otimes\widetilde{f}^{T_2^2}\otimes(\otimes_{t=1}^{2}(\widetilde{1}\ominus\widetilde{e}^{S_t^{(pr)T_2^2}}))\otimes\widetilde{d}_l^{T_2^2}\otimes(\otimes_{t=1}^{3}(\widetilde{1}\ominus\widetilde{e}^{S_t^{(pa)T_2^2}})),$$
$$\widetilde{R}_l^{T_1^3} = \widetilde{D'}(A_3, A_5)\otimes\widetilde{f}^{T_1^3}\otimes(\otimes_{t=1}^{4}(\widetilde{1}\ominus\widetilde{e}^{S_t^{(pr)T_1^3}}))\otimes\widetilde{d}_l^{T_1^3}\otimes(\otimes_{t=1}^{5}(\widetilde{1}\ominus\widetilde{e}^{S_t^{(pa)T_1^3}})),$$
$$\widetilde{R}_l^{T_1^4} = \widetilde{D'}(A_4, A_5)\otimes\widetilde{f}^{T_1^4}\otimes(\otimes_{t=1}^{4}(\widetilde{1}\ominus\widetilde{e}^{S_t^{(pr)T_1^4}}))\otimes\widetilde{d}_l^{T_1^4}\otimes(\otimes_{t=1}^{5}(\widetilde{1}\ominus\widetilde{e}^{S_t^{(pa)T_1^4}})),$$

where $\widetilde{D'}(A_i, A_5)$ is obtained from $\widetilde{D}(A_i, A_5)$ by multiplying the initial value of each arc by the reduction caused by the effect of failure transmission safeguards on that arc.

Table 2. Threats to the assets

Asset	Threat (T_j^i)	Frequency ($\widetilde{f}^{T_j^i}$)	Degradation ($\widetilde{\mathbf{d}}^{T_j^i}$)
A_1	T_1^1	H	(M, H, MH)
A_2	T_1^2	M	(H, M, MH)
A_2	T_2^2	H	(M, M, M)
A_3	T_1^3	MH	(H, H, M)
A_4	T_1^4	H	(H, MH, M)

Table 3. Risks to A_5 before applying the safeguards

Threat	Confidentiality	Integrity	Authenticity
T_1^1	(2898, 5622.7, 13449.1, 19500)	(6210, 10620.7, 23230.3, 30000)	(4554, 8121.7, 18339.7, 25500)
T_1^2	(2929.5, 5565.4, 13449.1, 19500)	(1367.1, 2946.4, 7786.3, 12675)	(2148.3, 4255.9, 10617.7, 16575)
T_2^2	(2929.5, 5565.4, 13449.1, 19500)	(2929.5, 5565.4, 13449.1, 19500)	(2929.5, 5565.4, 13449.1, 19500)
T_1^3	(3712.5, 7044.4, 17598.7, 25500)	(3712.5, 7044.4, 17598.7, 25500)	(1732.5, 3729.4, 10188.7, 16575)
T_1^4	(2362.5, 4876.9, 12905.7, 19500)	(1732.5, 3729.4, 10188.7, 16575)	(1102.5, 2581.9, 7471.7, 12675)

This optimization problem has $3\times5 = 15$ fuzzy risk elements in the objective function and $2^{(32+22+16)} = 1.18\times10^{21}$ possible solutions.

The initial solution considered in SA for solving this optimization problem consists of randomly generated packages of failure transmission, preventive and palliative safeguards. The total cost of the initial solution obviously has to be below 5000 to be feasible.

The neighborhood of a given solution x_i, $N(x_i)$, is composed of any solutions whose associated packages of safeguards differ by at most one safeguard randomly selected from x_i. If the resulting solution is not feasible, then it is discarded, and another solution is generated in the neighborhood until a feasible solution is found (associated costs ≤ 5000).

The initial temperature assures acceptance probabilities of worse solutions close to 0.9 in the initial iterations of the algorithm. The initial temperature is computed to obtain a high probability of acceptance (≥ 0.9) of any neighbor of the initial solution, i.e., given the initial solution x_0, the minimum value T is computed such that $e^{-(f(y)-f(x_0))/T_0} \geq 0.9, \forall y \in N(x_0)$. If we identify an upper bound for $(f(y) - f(x_0))$, i.e., $M \geq f(y) - f(x_0)$, then $T_0 = -M/\ln(0.9)$.

According to the Murakami ranking index, we can consider

$$M = max_{i,j,l}\{\mathbf{x}_{\widetilde{R}_l^{T^i}{}^j}\}, \tag{8}$$

which is obviously achieved when no safeguard is considered, leading to $M = 19077$ and $T_0 = 181064$.

The temperature is kept constant for $L = 20$ iterations and is then decreased after multiplying by 0.9, so that, after $h \cdot L$ iterations, the temperature is $T_{h \cdot L} = 0.9^h T_0$. The algorithm stops when there has been no improvement in the best solution over the last 30% of the total number of iterations.

Table 4. Failure transmission safeguards

Asset	Safeguards (Tag, Effect, Cost)
A_4	$S^{45} = \{(S_1^{45}, M, 205), (S_2^{45}, L, 124), (S_3^{45}, ML, 230), (S_4^{45}, M, 189),$ $(S_5^{45}, L, 104), (S_6^{45}, M, 167), (S_7^{45}, M, 178), (S_8^{45}, L, 98)\}$
A_3	$S^{35} = \{(S_1^{35}, M, 198), (S_2^{35}, L, 100), (S_3^{45}, M, 123), (S_4^{35}, M, 167),$ $(S_5^{35}, L, 89), (S_6^{35}, M, 178), (S_7^{35}, M, 209), (S_8^{35}, L, 100)\}$
A_2	$S^{25} = \{(S_1^{25}, M, 203), (S_2^{25}, M, 198), (S_3^{25}, L, 170)\}$
	$S^{23} = \{(S_1^{23}, L, 143), (S_2^{23}, M, 178), (S_3^{23}, M, 154), (S_4^{23}, M, 190), (S_5^{23}, L, 102)\}$
A_1	$S^{14} = \{(S_1^{14}, M, 178), (S_2^{14}, M, 160), (S_3^{14}, L, 120), (S_4^{14}, L, 105)\}$
	$S^{12} = \{(S_1^{12}, L, 120), (S_2^{12}, M, 180), (S_3^{12}, L, 104), (S_4^{12}, M, 200)\}$

Fig. 3 shows the fitness function trajectory of SA for this problem, in which the centroid of the maximum risk declines to 4044. Note that the centroid before the implementation of safeguards was 19077. Table 6 shows the solutions output, whose associated cost is 4850 monetary units, whereas Table 7 shows the new risk values once the selected safeguards are implemented.

If we compare the risk values for the terminal asset A_5 in Tables 3 and 7, i.e., before and after the implementation of the selected safeguards, we find that the risk reduction is significant. The maximum risk is associated with threat T_1^1 both before and after the implementation of the selected safeguards, but the sum of the centroids of each component are 48.560 and 10.373 monetary units, respectively.

Note that the risks for the whole IS are the same as for asset A_5, since it is the only terminal asset.

Table 5. Preventive and palliative safeguards

Palliative	Safeguards (Tag, Effect (C, I, A), Cost)
$S^{T_1^1 pa}$	$\{(S_1^{T_1^1 pa}, (H,H,H), 520), (S_2^{T_1^1 pa}, (M,L,M), 250), (S_3^{T_1^1 pa}, (L,L,VL), 100),$ $(S_4^{T_1^1 pa}, (ML,VL,L), 96), (S_5^{T_1^1 pa}, (VL,L,ML), 110), (S_6^{T_1^1 pa}, (ML,M,L), 78)\}$
$S^{T_1^3 pa}$	$\{(S_1^{T_1^3 pa}, (H,H,H), 535), (S_2^{T_1^3 pa}, (L,L,VL), 89), (S_3^{T_1^1 pa}, (H,H,H), 670),$ $(S_4^{T_1^3 pa}, (ML,H,L), 537), (S_5^{T_1^3 pa}, (H,L,ML), 477)\}$
$S^{T_1^2 pa}$	$\{(S_1^{T_1^2 pa}, (H,H,H), 496), (S_2^{T_1^2 pa}, (VL,L,ML), 110), (S_3^{T_1^2 pa}, (ML,M,L), 78)\}$
$S^{T_2^2 pa}$	$\{(S_1^{T_2^2 pa}, (M,L,M), 195), (S_2^{T_2^2 pa}, (L,L,VL), 89), (S_3^{T_2^2 pa}, (ML,VL,L), 56)\}$
$S^{T_1^4 pa}$	$\{(S_1^{T_4^3 pa}, (H,H,H), 539), (S_2^{T_1^4 pa}, (L,L,VL), 110), (S_3^{T_1^4 pa}, (ML,H,L), 478),$ $(S_4^{T_1^4 pa}, (ML,H,L), 495), (S_5^{T_1^4 pa}, (H,H,H), 689)\}$
Preventive	**Safeguards (Tag, Effect, Cost)**
$S^{T_1^1 pr}$	$\{(S_1^{T_1^1 pr}, H, 367), (S_2^{T_1^1 pr}, H, 485), (S_3^{T_1^1 pr}, ML, 100), (S_4^{T_1^1 pr}, ML, 120)\}$
$S^{T_1^3 pr}$	$\{(S_1^{T_1^3 pr}, M, 198), (S_2^{T_1^3 pr}, L, 100), (S_3^{T_1^1 pr}, M, 123), (S_4^{T_1^3 pr}, M, 167)\}$
$S^{T_1^2 pr}$	$\{(S_1^{T_1^2 pr}, M, 203), (S_2^{T_1^2 pr}, M, 198)\}$
$S^{T_2^2 pr}$	$\{(S_1^{T_2^2 pr}, M, 178), (S_2^{T_2^2 pr}, M, 160)\}$
$S^{T_1^4 pr}$	$\{(S_1^{T_4^3 pr}, M, 178), (S_2^{T_1^4 pr}, M, 160), (S_3^{T_1^4 pr}, L, 120), (S_4^{T_1^4 pr}, L, 105)\}$

Table 6. Final selection of failure transmission, preventive and palliative safeguards

Arc	Failure transmission safeg.	Threat	Preventive safeg.	Palliative safeg.
(A_4, A_5)	(10100111)	T_1^1	(0011)	(000011)
(A_3, A_5)	(10111110)	T_1^2	(00)	(110)
(A_2, A_5)	(110)	T_2^2	(00)	(101)
(A_2, A_3)	(01111)	T_1^3	(0010)	(00000)
(A_1, A_4)	(0100)	T_1^4	(0100)	(00000)
(A_1, A_2)	(0101)			

Table 7. Risks to A_5 after the implementation of the selected safeguards

Threat	Confidentiality	Integrity	Authenticity
T_1^1	(16.9, 161.72, 936.2, 3681.5)	(32.70, 239.7, 1295.6, 5197.4)	(25.1, 198.6, 1576.7, 5777.1)
T_1^2	(0, 49.6, 458.1, 1791.2)	(0, 29.7, 289.7, 1397.1)	(0, 24.6, 352.6, 1552.9)
T_2^2	(0, 49.6, 458.1, 1791.2)	(0, 29.7, 289.7, 1397.1)	(76, 379.3, 2074.3, 5588.4)
T_1^3	(12.2, 110.5, 647.2, 2465.6)	(21.9, 147.3, 744.3, 2958.7)	(6.8, 58.5, 487.1, 1923.2)
T_1^4	(34.8, 245.5, 1176.8, 3793.2)	(62.7, 327.4, 1353.3, 4551.9)	(19.5, 129.9, 885.7, 2958.7)

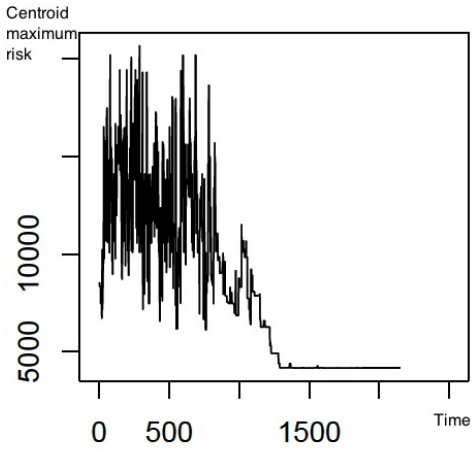

Fig. 3. Centroid of the maximum risk evolution

5. Conclusions

The selection of failure transmission, preventive and palliative safeguards that minimize the maximum risk caused by threats to the assets of an information system (IS) for a given budget is a combinatorial optimization problem, which has to be solved by means of a metaheuristic.

Moreover, we have assumed that all the elements in the IS risk analysis can be rated using linguistic terms with associated normalized fuzzy numbers. This is less stressful on experts and useful for accounting for imprecision and/or vagueness concerning the elements. However, this involves the inclusion of fuzzy elements in the optimization problem, such as the ranking of fuzzy numbers to derive a total order in the objective function. We have modeled this optimization problem, which we have solved by means of simulated annealing.

As discussed in the paper, assignments based on a rigid linguistic term scale is not always advisable since the expert has no say in the number of linguistic terms that the scale is to include and about the appearance of their associated trapezoidal fuzzy numbers. This could be considered as a limitation of the proposed approach. However, we have alternatively proposed the use of a betting and lottery-based method for fuzzy probability elicitation. In the future, we intend to work on procedures for building a linguistic term scale that represents the expert's preferences.

Besides, we have assumed that the threat frequencies are represented by linguistic terms (trapezoidal fuzzy numbers). However, these frequencies might change depending on a number of variables in the context of the IS. In the future we intend to build a fuzzy control system to establish different alarm levels according to these variable values.

Acknowledgments. The paper was supported by Madrid Government project S-2009/ESP-1685 and the Ministry of Science project MTM2011-28983-CO3-03 and MTM2014-56949-C3-2-R.
This paper is an extension of reference [26] presented at the 2014 World Conference on Information Systems and Technologies (WorldCIST'14) in Madeira (Portugal), January 2014.

References

1. Bortolan, G., Degani R.: A Review of Some Methods for Ranking Subsets. Fuzzy Sets and Systems, Vol. 15, 1-19 (1985)
2. Brunelli, M., Mezei, J.: How Different are Ranking Methods for Fuzzy Numbers? A Numerical Study. International Journal of Approximate Reasoning, Vol. 54, 627-639 (2013)
3. CCTA Risk Analysis and Management Method (CRAMM), Version 5.0. Central Computing and Telecommunications Agency (CCTA), London, UK. (2003)
4. Cerny, V.: Thermodynamical Approach to the Traveling Salesman Problem: An Efficient Simulation Algorithm. Journal of Optimization Theory and Applications, Vol. 45, 41-51 (1985)
5. Chen, S.-J. and Chen, S.-M. Fuzzy Risk Analysis Based on Similarity Measures of Generalized Fuzzy Numbers, *IEEE Transactions on Fuzzy Systems*, vol. 11, pp. 45–56. (2003)
6. Chen, S.-J. and Chen, S.-M. Fuzzy Risk Analysis Based on the Ranking of Generalized Trapezoidal Fuzzy Numbers, *Applied Intelligence*, vol. 26, pp. 1–11 (2007).
7. Finetti, B., Foresight: its logical laws, its subjective sources. In: Studies in Subjective Probability. Wiley, New York, USA. (1964)
8. Hejazi S.R., Doostparast, A. and Hosseini, S. M., An improved fuzzy risk analysis based on a new similarity measures of generalized fuzzy numbers. Expert Systems with Applications: An International Journal. Vol. 38 9179-9185 (2011)
9. ISO/IEC 17799:2005, Information Technology - Security Techniques - Code of Practice for Information Security Management. International Organization for Standardization, Geneva, Switzerland. (2005)
10. ISO/IEC 27000:2009, Information Security Management Systems — Overview and Vocabulary. Geneva, Switzerland (2009)
11. ISO/IEC 27001:2005, Information technology — Security Techniques — Information Security Management Systems - Requirements. Geneva, Switzerland (2005)
12. ISO/IEC 27005:2011, Information Technology - Security Techniques - Information Security Risk Management. International Organization for Standardization, Geneva, Switzerland. (2011)
13. Halliwell, J., Keppens, J., Shen, Q. Linguistic bayesian networks for reasoning with subjective probabilities in forensic statistics. In Proceedings of the 9th International Conference on Artificial Intelligence and Law, pages 4250 (2003)
14. Herrera, F., Martnez, L. A 2-tuple fuzzy linguistic representation model for computing with words. IEEE Transactions on Fuzzy Systems, 8(6):746–752 (2000).
15. Kirkpatrick, S., Gelatt, C. D., Vecchi, C. D.: Optimization by Simulated Annealing. Science, Vol. 220, 671-680. (1983)
16. López Crespo, F., Amutio-Gómez, M. A., Candau, J., Mañas, J. A.: Methodology for Information Systems Risk. Analysis and Management (MAGERIT version 2). Books I, II and III. Ministerio de Administraciones Públicas, Madrid, Spain. (2006).
17. Lee, M.C. Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method. International Journal of Computer Science & Information Technology Vol 6, No 1 (2014)
18. Murakami, S., Maeda, S., Imamura, S.: Fuzzy Decision Analysis on the Development of Centralized Regional Energy Control System. In: IFAC Symposium on Fuzzy Information Knowledge Representation and Decision Analysis. Pergamon Press, New York, USA, 363-368. (1983)
19. Savage, L.J., The Fundations of Statistics. Wiley, New York, USA. (1954)
20. Stoneburner, G., Gougen, A.: NIST 800-30 Risk Management. Guide for Information Technology Systems. National Institute of Standard and Technology, Gaithersburg, USA. (2002)
21. Vicente, E., Jiménez, A., Mateos, A.: A Fuzzy Approach to Risk Analysis in Information Systems. In: Proceedings of the 2nd International Conference on Operations Research and Enterprise Systems, Scitepress, Barcelona, Spain, 130-133. (2013)

22. Vicente, E., Jiménez, A., Mateos, A.: An Interactive Method of Fuzzy Probability Elicitation in Risk Analysis, In: Intelligent Systems and Decision Making for Risk Analysis and Crisis Response, CRC Press, New York, USA, 223-228. (2013)
23. Vicente, E., Mateos, A., Jiménez, A.: A New Similarity Function for Generalized Trapezoidal Fuzzy Numbers, In: Artificial Intelligence and Soft Computing, Lecture Notes in Artificial Intelligence, Vol. 7894, Springer, Berlin, Germany, 400-411. (2013)
24. Vicente, E., Mateos, A., Jiménez, A.: Similarity Functions for Generalized Trapezoidal Fuzzy Numbers: An Improved Comparative Analysis. Journal of Intelligent and Fuzzy Systems, Vol. 28, 821-833 (2015)
25. Vicente, E., Mateos, A., Jiménez-Martín, A. A Fuzzy Approach based on Dynamic Programming and Metaheuristics for Selecting Safeguards for Risk Management for Information Systems. In: Proceedings of the 3rd International Conference on Operations Research and Enterprise Systems, Scitepress, Angers, France, 35-46. (2014)
26. Vicente, E., Mateos, A., Jiménez-Martín, A. Selection of Safeguards for Fuzzified Risk Management in Information Systems. In: New Perspectives in Information Systems and Technologies, Advances in Intelligent Systems and Computing, Vol. 275, Springer, Berlin, Germany, 267-276. (2014)
27. Vicente, E., Mateos, A., Jiménez-Martín, A. Risk Analysis in Information Systems: A Fuzzification of the MAGERIT Methodology. Knowledge-Based Systems, Vol. 66, 1-12. (2014).
28. Wei, S. H., Chen, S. M. A New Approach for Fuzzy Risk Analysis Based on Similarity Measures of Generalized Fuzzy Number, Expert Systems with Applications, vol. 36, pp. 589–598 (2009)
29. Wang, X., Kerre, E. E.: Reasonable Properties for the Ordering of Fuzzy Quantities (I and II), Fuzzy Sets and Systems, Vol. 118, 375-385. (2001)
30. Xu, Z., Shang, S., Qian, W., Shu, W.: A Method for Fuzzy Risk Analysis based on the New Similarity of Trapezoidal Fuzzy Numbers. Expert Systems with Applications, Vol. 37, 1920-1927 (2010)
31. Xu, Z.S. A method based on linguistic aggregation operators for group decision making with linguistic preference relations. Information Science, 166:19–30, 2004.
32. J. Wang and J. Hao. A new version of 2-tuple fuzzy linguistic representation model for computing with words. IEEE transactions on fuzzy systems, 14:435–445,
33. Zadeh, L. A.: Fuzzy Sets. Information and Control, Vol. 8, 338-353. (1965)
34. Zadeh. L. A.: The Concept of a Linguistic Variable and its Application to Approximate Reasoning. Parts 1, 2 and 3. Information Sciences, Vol. 8, 199-249. (1975)
35. Zain, N.M., Samy, G.N., Zuraini, R.A., Manaf, A.A. Fuzzy Based Threat Analysis in Total Hospital Information System. Advances in Computer Science and Information Technology Lecture Notes in Computer Science Volume 6059, 2010, pp 1-14 (2010)
36. Zhu, L., Xu, R. Fuzzy Risk Analysis based on Similarity Measure of Generalizard Fuzzy Numbers. Fuzzy Enginering and Operations Research. Berlin/Heidelberg: Springer, 569-587 (2012)

D. Eloy Vicente Cestero obtained a degree in Mathematics from the Universidad de Extremadura in 2009, a degree in Applied Statistics form the Universidad Nacional de Educación a Distancia, a MSc in Decision Systems Engineering from the Universidad Rey Juan Carlos, a MSc in Artificial Intelligence from the Department of Artificial Intelligence (Universida Politécnica de Madrid). At the present time, he is a PhD student of Artificial Intelligence at the University Politécnica de Madrid and he is working in Sopra Group.

His research lines are Decision Sciences, Risk Analysis, Statistics and Operational Research and Big Data. He has written more than 10 papers (3 of them listed in JCR), such as Knowledge-based Systems, Computer Science and Information Systems or Journal of

Intelligent & Fuzzy Systems. He has participated in 2 research projects and was reader of a paper 4 times in conferences.

Prof. Dr. Alfonso Mateos Caballero is an Associate Professor of Statistics and Operations Research at the Artificial Intelligence Department (ETSI Informática, Universidad Politécnica de Madrid). He is director of the Decision Analysis and Statistics Group. All his professional life has been related to Operations Research, Statistics, Decision Analysis and Decision Support Systems. He has written more than 120 papers in Spanish and International journals (20 of them listed in JCR), such as EJOR, Computational Optimization and Applications, Annals of Operations Research, JORS, Reliability Engineering and System Safety, DSS, GDN, Computers & Operations Research, OMEGA or Knowledge-based Systems. He has directed 5 and has participated in more than 26 projects (4 of them are European Projects), has co-authored 5 books and was reader of a paper more than 125 times in conferences.

His research is currently involved in the development of Intelligent Decision Support Systems based on Bayesian forecasting and time series analysis, influence diagrams and multi-attribute utility theory, with applications in price forecasting in the Spanish electric market, extracorporeal life support (medicine), restoring radionuclide contaminated fresh water ecosystem (environment) and valuation forecasting of real estate, risk analysis and management and Big Data.

Antonio Jiménez-Martín gained degree in Computer Science from Universidad Politécnica de Madrid. Spanish Royal Academy of Doctors Research Award 2003 (Experimental and Technological Sciences Section). He is Associated Professor of Operations Research and Simulation. His research interest are multi criteria decision-making, risk analysis and management, simulation methods and metaheuristics, and group decision-making, and is involved in the development and implementation of decision support systems based on multi-attribute utility theory. He has written more than 100 papers in International journals (21 of them listed in JCR), and participated in than 29 research projects (7 of them are European Projects), co-authored 4 books and was reader of a paper more than 125 times in conferences.

Received: September 25, 2014; Accepted: May 21, 2015.