Expert Systems with Applications 37 (2010) 3561–3573

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

Fuzzy integrated vulnerability assessment model for critical facilities in combating the terrorism

Ilker Akgun [a,*], Ahmet Kandakoglu [a], Ahmet Fahri Ozok [b]

[a] Department of Industrial Engineering, Management Faculty, Istanbul Technical University, 34367 Macka, Istanbul, Turkey
[b] Industrial Engineering Department, Istanbul Kültür University, 34156 Bakırköy, Istanbul, Turkey

ARTICLE INFO

Keywords:
Airport
Fuzzy Cognitive Maps (FCM)
Fuzzy integrated vulnerability assessment model (FIVAM)
Fuzzy set theory
Interdependency
Simple Multi-Attribute Rating Technique (SMART)
Terrorism

ABSTRACT

Critical facility vulnerability assessment is a highly complex strategic activity in combating the terrorism and necessitates a structured quantified methodology to support the decision-making process in defense planning. In the system perspective, the critical facility, such as airport, dam, governmental facility, harbor, nuclear power plant, oil plant etc., can be defined as a system that relies on a group of different interdependent logical and physical entities as system functions and system components.

The aim of this paper is to present a realistic approach to determine the vulnerability of such a system defended against the terrorist attack under multiple criteria which can be both qualitative and quantitative by considering these interdependencies. The proposed approach, called fuzzy integrated vulnerability assessment model (FIVAM), is based on fuzzy set theory, Simple Multi-Attribute Rating Technique (SMART) and Fuzzy Cognitive Maps (FCM) methodology in a group decision-making environment. The FIVAM approach is presented step-by-step and applied to a simple case study on airport vulnerability assessment. The results of the application are compared to those observed through a classical vulnerability assessment model to illustrate the effectiveness of the FIVAM. Furthermore, FIVAM provides a framework to identify the hidden vulnerabilities caused by the functional interdependencies within the system. The results also show that FIVAM quantifies the vulnerability of the system, system functions and system components, and determines the most critical functions and components by simulating the system behavior.

1. Introduction

Although there is no internationally agreed definition of terrorism, it is generally defined as "the unlawful use or threatened use of force or violence by a person or an organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons" (Mifflin, 2006). Terrorism includes intelligent, deliberate, and unpredictable acts which are intended to create fear, are committed for an ideological goal, and deliberately target or disregard the safety of civilians. Thus, combating the terrorism is fundamentally different from conventional war, natural disasters, and criminal acts and has to be handled in a different way.

For combating the terrorism, vulnerability assessment of a system defended against terrorist attack is initial and crucial step (Garrick et al., 2004; Sarewitz, Pielke, & Keykhah, 2003). Vulnerability can be defined as a "weakness in the system defended" in a most common and simplest way. Indeed, more vulnerable means easier to be damaged or harmed. Although a comprehensive list of vulnerability definitions can be found in Ezell (2007), the term vulnerability still remains as a vague term. Therefore, a workable definition of vulnerability is especially difficult to formulate and quantify. Vulnerability must be quantifiable so that vulnerability assessment before terrorist attack occurs can be done. Vulnerability assessment is a systematic process of identification and evaluation of system vulnerabilities (Garrick et al., 2004). Firstly, vulnerability assessment is intended to identify the weaknesses of a system that terrorists can exploit. Then, vulnerabilities that are most significant are evaluated and focused on. It may be impractical or usually even impossible to eliminate all system vulnerabilities because of time and resource constraints. It is required to be aware of these vulnerabilities for developing the necessary defense methods and for assigning the defense resources consistently.

Critical facilities are the systems that have a high impact to the psychology, health and welfare of the population, and are essential to the operations of the economy and government such as airport, dam, governmental facility, harbor, nuclear power plant and oil plant. Hence, critical facilities are attractive targets for terrorist attacks and should be given special consideration for vulnerability assessment. As critical facilities are complex both topologically and functionally, critical facility vulnerability assessment is a challenging issue. Each critical facility as a system contains some degree of vulnerability and vulnerabilities may have different

* Corresponding author. Tel.: +90 212 293 1300x2073; fax: +90 212 240 7260.
E-mail address: akguni@itu.edu.tr (I. Akgun).

0957-4174/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2009.10.035

effects on the system and its functions/services. System functions are addressed as purposeful actions that system components contribute to accomplish system mission. System functions are not physical entities like system components and the dependence between system functions and system components, physical dependencies, is frequently difficult to assess accurately. In addition to this, system functions are not independent of each other. Because of high degree of uncertainties, it is also difficult to discover quantitative and precise information on system function interdependencies. Interaction among system functions produces the emergence of complex relationships that are not predictable by the knowledge of any single system function. Designing a realistic vulnerability assessment necessitates consideration of complex causal relationships among various system functions, logical dependencies. Both the presence of either hidden or poorly understood interdependencies and their cascading effects are required to be handled. Previous studies on this issue have largely ignored the possible interrelationships among the system functions that affect the system state.

It is extremely difficult in terrorism case to obtain exact data under uncertainty against an adversarial and adaptive opponent. Much of the information related to vulnerability assessment is not quantitative. Rather, this incomplete and imprecise information is expressed qualitatively as words or phrases in a natural language by experts of different fields such as terrorism experts, security experts, engineers, and academicians. Individual opinions, evaluations and ratings from these experts must be identified and applied to vulnerability assessment. Vulnerability assessment problem can be recognized as a group decision-making (GDM) problem under multiple criteria. Therefore, there is a value in considering fuzzy set theory and GDM methods for critical facility vulnerability assessment.

The purpose of this study is to present a fuzzy integrated vulnerability assessment model (FIVAM) based on fuzzy SMART and FCM techniques to assess the vulnerability of a critical facility in the GDM environment. The proposed FIVAM approach enables to determine the vulnerability values under multiple criteria as well as provides a framework to simulate the system vulnerability behavior depending on the vulnerabilities of the interdependent system functions. Additionally, FIVAM allows the decision makers to identify the hidden vulnerabilities caused by the functional interdependencies within the system.

The remainder of this paper is organized as follows: Section 2 overviews the existing approaches and the factors that influence the system vulnerability assessment. In Section 3, fundamentals of fuzzy set theory, the theoretical framework of SMART and the principles of FCM are represented. The proposed FIVAM and its process flow are introduced in Section 4. The illustrative application of FIVAM is performed over an airport case study in Section 5. This section also examines the utility of findings and discusses the analysis results. Conclusions and further issues are addressed respectively in the final section.

2. Literature review on vulnerability assessment

There is confusion in the terms ‘‘vulnerability” and ‘‘risk” as applied to combating the terrorism in the literature. To overcome this issue, Ezell (2007) presented a relationship emerging between vulnerability and risk. According to his study, vulnerability highlights the notion of susceptibility to a scenario, whereas risk focuses on the severity of consequences within the context of a scenario. In addition to this, Willis (2007) defined terrorism risk as a function of threat, vulnerability and consequences. Vulnerability assessment is generally employed as a sub process of risk analysis in the previous studies (Garrick et al., 2004).

Recently, vulnerability assessment has gained a dynamic and complex nature, and become an active area of research due to its increasing strategic significance in various application areas. However, the focus of this study is limited to the researches for critical facility vulnerability assessment in combating the terrorism. This survey also incorporates the studies for critical infrastructures vulnerability assessment briefly, as critical facilities rely on these critical infrastructures and have some key critical infrastructure components together with system specific components within their system bounds. The critical infrastructures can be defined as a complex set of interconnected, interdependent, geographically dispersed systems on which the nation depend as energy distribution, telecommunications, rail, water supply networks, etc.

In the literature, there have been several approaches for vulnerability assessment and these approaches can be categorized into two main groups as follows: qualitative approaches and quantitative approaches. Qualitative approaches are generally applied in the sub process of the risk assessment studies (Bajpai & Gupta, 2007). Despite the increasing significance of vulnerability assessment in combating the terrorism, researches and analyses using quantitative methodologies have been rarely seen in the literature.

Bajpai and Gupta (2005) have shown that security risk status of oil and gas facilities can be assessed qualitatively by developing a security risk factor table and vulnerability assessment worksheet. They divided the facility into various zones and identified the factors that influence the overall security of the facility by rating them on a scale from 0 to 5. Qualitative methods as in Bajpai and Gupta (2005) permit vulnerability ranking or separation into descriptive categories of vulnerability (Garrick et al., 2004). Therefore, qualitative methods can be used to pre-assess the vulnerability but much more is required to quantify the vulnerability.

Generally, existing quantitative methodology studies focused on one kind of critical infrastructure such as energy (Salmeron, Wood, & Baldick, 2004), telecommunications (Murray, Matisziw, & Grubesic, 2007), water system (Ezell, 2007), etc. Salmeron et al. (2004) developed a max–min model to determine the weaknesses in the electric grid to prepare for terrorist attacks. Through decomposition, they solved the problem with a heuristic on two test systems. Murray et al. (2007) presented an optimization approach for identifying interdiction bounds with respect to connectivity and/or flow associated with a system of origins and destinations. They applied this approach to the telecommunications flow in United States. Apostolakis and Lemon (2005) used Multi-Attribute Utility Theory (MAUT) for the identification and prioritization of vulnerabilities in an infrastructure that they modeled using interconnected digraphs and employed graph theory to identify the candidate vulnerable scenarios. Ezell (2007) proposed an Infrastructure Vulnerability Assessment Model (I-VAM) based on MAUT and applied it to a medium-sized clean water system. In this model, the system is presented in a hierarchical structure and clean water system model decomposition serves as the structure of the value model with deterrence, detection, delay, and response value functions used to measure protection for components of the system.

There are also various studies that models critical infrastructure interdependencies. Brown, Beyeler, and Barton (2004) applied simulation to study the impacts of disruptions and used risk analysis to assess infrastructure interdependencies. Their purpose was to identify infrastructure risks and ways to reduce them. Min, Beyeler, Brown, Son, and Jones (2007) proposed a modeling and analysis framework that uses system dynamics, functional models and nonlinear optimization algorithms to study the entire interconnected system of infrastructures. Their purpose was to simulate the effects of localized capacity losses on the entire integrated system and to predict the extent of the shortage and its impact across the entire system.

From the previous researches, it is observed that vulnerability assessment in combating the terrorism is recognized as a worldwide problem. Despite the availability of the researches on this issue, the nature of the problem additionally seeks for the utilization of fuzzy logic in order to deal with the uncertainty and the vagueness of the decision environment in practice. Furthermore, in addition to the physical dependencies of the system functions, the interdependencies among the system functions, logical dependencies, in other words logical vulnerabilities, have to be considered and included into the vulnerability computations. Quantifying the vulnerability of such a system defended against the terrorist attack by considering the interdependencies among the functions of the system has not been adequately addressed in the literature. That is why; these existing approaches and decision-making models are not satisfying the solution of this problem in a consistent manner. Hence, this paper addresses a quantified fuzzy approach based on SMART and FCM methodology for managing a more realistic and structured vulnerability assessment process to provide practical solutions in real life applications.

3. Theoretical background

In this section, theoretical background information on triangular fuzzy numbers (TFNs), linguistic variables, fuzzy SMART and FCM methodologies are presented, respectively.

3.1. Triangular fuzzy number (TFN)

A fuzzy number is a convex, normalized fuzzy set defined on the real line whose membership function is at least semi continuous and has the functional value $\mu_{\widetilde{M}}(x) = 1$ at precisely one element (Ross, 1995). In other words, a fuzzy number is a quantity whose value is imprecise rather than exact. Among the various types of a fuzzy number such as trapezoidal, bell-shaped, etc., TFN is the most popular one as it is easy to use and interpret. A TFN is completely represented by a triplet such as $\widetilde{M} = (a|b, b|c)$ or $\widetilde{M} = (a, b, c)$ whose membership function can be defined as (Kaufmann & Gupta, 1991)

$$\mu_{\widetilde{M}}(x) = \begin{cases} 0, & x < a, \\ \frac{(x-a)}{(b-a)}, & a \leqslant x \leqslant b, \\ \frac{(c-x)}{(c-b)}, & b \leqslant x \leqslant c, \\ 0, & x > c. \end{cases} \quad (1)$$

The parameters a, b and c, respectively, denote the smallest possible value, the most promising value, and the largest possible value that describe a fuzzy event. A sample TFN, $\widetilde{M} = (a, b, c)$, is shown in Fig. 1.

The fuzzy algebraic operations (addition, multiplication, division and subtraction) of two TFNs $\widetilde{M}_1 = (a_1, b_1, c_1)$ and $\widetilde{M}_2 = (a_2, b_2, c_2)$ are applied as expressed within the contents of various researches (Chen & Hwang, 1992; Kaufmann & Kaufmann, 1991).

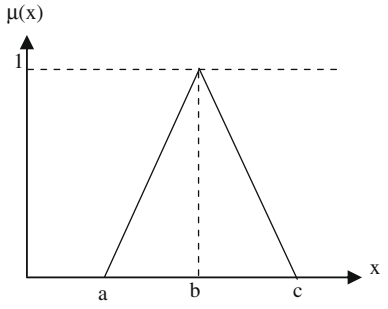

Fig. 1. A triangular fuzzy number, $\widetilde{M} = (a, b, c)$.

The result of fuzzy operations is a fuzzy number and in some situations a single scalar quantity is needed as an output. Therefore, it is required to convert a fuzzy number into a crisp value. There are several available defuzzification methods for this purpose in the literature. Mean of maximum (MOM), centroid method (or center of area – COA) and α-cut methods are the most common defuzzification methods (Lee, 1990; Sugeno, 1985). Each of these methods has advantages and disadvantages. In this study, the centroid method is utilized due to its simplicity and widespread use. A TFN, $\widetilde{M} = (a, b, c)$, is defuzzified by using the following centroid method equation:

$$D(\widetilde{M}) = \frac{\int_a^c x\mu_{\widetilde{M}}(x)dx}{\int_a^c \mu_{\widetilde{M}}(x)dx} = \frac{\int_a^c \left(x \cdot \frac{x-a}{b-a}\right)dx + \int_b^c \left(x \cdot \frac{c-x}{c-b}\right)dx}{\int_a^c \left(\frac{x-a}{b-a}\right)dx + \int_b^c \left(\frac{c-x}{c-b}\right)dx} = \frac{1}{3}(a+b+c). \quad (2)$$

3.2. Linguistic variables

A linguistic variable is a variable whose values are words or sentences in a natural or artificial language (Zadeh, 1975). According to Zadeh (1975), it is very difficult for conventional quantification to express reasonably those situations that are overtly complex or hard to define; thus, the notion of a linguistic variable is necessary in such situations. Since linguistic variables are not directly mathematically operable, each linguistic variable is associated with a fuzzy number characterizing the meaning of each generic verbal term. In fuzzy set theory, conversion scales are applied to transform linguistic terms into fuzzy numbers. Determining the number of conversion scales is generally intuitive (Chen & Hwang, 1992).

Since the use of fuzzy logic becomes very important for the decision-making problem in this study, linguistic variables are used to express the qualitative judgments such as the relative importance weights of vulnerability criteria, component and function dependency values, the ratings of system components, and the degree of influence (or causal relationships) among system functions. The possible values for these variables are presented in Tables 1–3. For example, the decision makers are asked to describe the degree of influence among system functions using a linguistic variable given in Table 3 and each linguistic variable is indicated by a TFN within the interval of [0, 1]. The linguistic variables in Table 3 and their membership functions are shown in Fig. 2.

Table 1
Linguistic variables for the relative importance weights and dependency values.

Linguistic variable	Triangular fuzzy number
Very low (VL)	(0, 0, 0.1)
Low (L)	(0, 0.1, 0.3)
Medium low (ML)	(0.1, 0.3, 0.5)
Medium (M)	(0.3, 0.5, 0.7)
Medium high (MH)	(0.5, 0.7, 0.9)
High (H)	(0.7, 0.9, 1)
Very high (VH)	(0.9, 1, 1)

Table 2
Linguistic variables for the ratings of system components.

Linguistic variable	Triangular fuzzy number
Very poor (VP)	(0, 0, 1)
Poor (P)	(0, 1, 3)
Medium poor (MP)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Medium good (MG)	(5, 7, 9)
Good (G)	(7, 9, 10)
Very good (VG)	(9, 10, 10)

Table 3
Linguistic variables for causal relationships among system functions.

Linguistic variable	Membership function	Triangular fuzzy number
Very very low (VVL)	μ_{vvl}	(0, 0.1, 0.2)
Very low (VL)	μ_{vl}	(0.1, 0.2, 0.35)
Low (L)	μ_{l}	(0.2, 0.35, 0.5)
Medium (M)	μ_{m}	(0.35, 0.5, 0.65)
High (H)	μ_{h}	(0.5, 0.65, 0.8)
Very high (VH)	μ_{vh}	(0.65, 0.8, 0.9)
Very very high (VVH)	μ_{vvh}	(0.8, 0.9, 1)

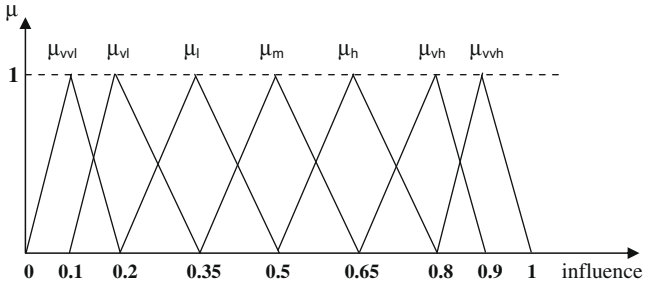

Fig. 2. Membership functions of linguistic variables for causal relationships.

Besides the decision makers' qualitative judgments, the TFN can also be used to represent the quantitative terms. For example, "approximately equal to 30" can be represented by (29, 30, 31); "approximately between 20 and 24" can be represented by (20, 22, 24); the crisp number 10 can be represented by (10, 10, 10) as a special TFN for the fuzzy algebraic operations (Liang, 1999).

3.3. The fundamentals of SMART

SMART is a compensatory method of multiple criteria/attribute decision making (MCDM), developed by Edwards in 1971. This method was designed to provide a simple way to implement the beginnings of MAUT. SMART uses the Simple Additive Weight (SAW) method as a basis for obtaining the total values of individual alternatives to rank them according to the order of preference (Edwards, 1971, 1977; Edwards & Barron, 1994).

In this method, a score is obtained by adding the contribution from each criterion. Since two items with different measurement units cannot be added, normalization is required to permit addition among criteria values. The total score for each alternative can be computed by multiplying the normalized value of each criterion for the alternatives with the importance weight of the criterion and then summing these products over all the criteria (Yoon & Hwang, 1995). Formally, the total score of an alternative can be expressed as

$$S_i = \sum_{j=1}^{n} w_j r_{ij}, \quad i = 1, 2, \ldots, m, \tag{3}$$

where S_i is the total score of alternative i, w_j is the importance weight of criterion j, r_{ij} is the normalized rating of the alternative i for the criterion j, m is the number of alternatives and n is the number of criteria. Finally, the alternative with the highest score is selected as the preferred one.

In SMART, weights of criteria and ratings of alternatives are assigned directly using different scales. The simplicity of the questions done to the decision maker and the easiness of the analysis done on the answers are the great advantages of SMART. These issues directly influence on the understanding of the decision maker about the process used in the solution of the problem.

Another advantage of the SMART is that the decision model is independent of the alternatives (Brownlow & Watson, 1987). Since the ratings of alternatives are not relative, changing the number of alternatives considered will not in itself change the decision scores of the original alternatives (Edwards & Barron, 1994). This issue is particularly useful when new alternatives or criteria are needed to be added to the existing decision model. In that case, the evaluation process does not require any further evaluations and can continue from the previous scores obtained.

Furthermore, as the time is a crucial factor for managerial decision making, SMART becomes a better method than the other MCDM methods as it often requires a short period of decision cycle.

Along the years, the SMART has been successfully applied to various MCDM problems and became very popular as its analysis incorporates a wide variety of quantitative and qualitative criteria. Due to many advantages mentioned above, SMART becomes a better choice to evaluate the initial vulnerability of system components, system functions and the system with respect to determined criteria, and to deal with the ratings of both qualitative and quantitative criteria. Hence, in this study, a fuzzy SMART approach proposed by Chou and Chang (2008) in the GDM situation to solve a strategic MCDM problem is utilized.

3.4. Brief overview on FCM methodology

FCM methodology is a natural extension to cognitive maps, which can be found in the fields of economics, sociology and political science (Axelrod, 1976; Kosko, 1986). It is originated from the combination of Fuzzy Logic and Neural Networks for modeling complex systems. A FCM describes the behavior of a system in terms of concepts; each concept represents an entity, a state, a variable or a characteristic of the system (Dickerson & Kosko, 1997). FCMs are used to represent and to model the knowledge on the examining system. Existing knowledge on the behavior of the system is stored in the structure of nodes and interconnections of the map. The graphical illustration of an FCM is a signed fuzzy graph with feedback, consisting of nodes and weighted interconnections. Signed and weighted arcs connect various nodes representing the causal relationships that exist among concepts. A simple graphical representation of FCMs is depicted in Fig. 3.

In Fig. 3, C_i is a concept with a state value. The state value can be a fuzzy value within [0, 1] that represents the existent degree of a concept. The weight W_{ij} of an arrow indicates the influence degree from the cause concept C_i to the effect concept C_j, which can be a fuzzy value within $[-1, 1]$. Positive or negative sign and fuzzy weights (e.g. W_{12}) model the expert knowledge of the causal relationships (Kosko, 1991). Concept C_i causally increases C_j if the weight value $W_{ij} > 0$ and causally decreases C_j if $W_{ij} < 0$. When $W_{ij} = 0$; concept C_i has no causal effect on C_j. In practice, the sign of W_{ij} indicates whether the relationship between concepts is positive or negative, while the value of W_{ij} indicates how strongly concept C_i influences concept C_j. The forward or backward direction of

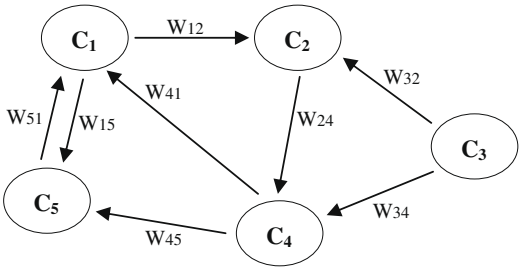

Fig. 3. A simple Fuzzy Cognitive Map.

causality indicates whether concept C_i causes concept C_j or vice versa, respectively.

The value of each concept in iterations can be computed from the values of the concepts in the preceding state using the following equation (Xirogiannis, Stefanou, & Glykas, 2004):

$$C_i^{t+1} = f\left(C_i^t + \sum_{j=1, j\neq i}^{n} W_{ji} C_j^t\right), \quad (4)$$

where C_i^{t+1} is the value of concept C_i at the step $t+1$, C_i^t is the value of the interconnected concept C_j at step t, W_{ji} is a corresponding fuzzy weight between two given nodes, from C_j to C_i and f is a given threshold function that transforms the result into a value in the interval where concepts can take values. The threshold function f can be bivalent ($f(x) = 0$ or 1), trivalent ($f(x) = -1$, 0 or 1), tangent hyperbolic ($f(x) = tanh(x)$) or the unipolar sigmoid function ($f(x) = 1/(1+e^{-\lambda x})$, where λ is a constant). Hyperbolic function is used when concepts can be negative and their values belong to the interval $[-1, 1]$. The unipolar sigmoid function where $\lambda > 0$ determines the steepness of the continuous function and is used when the values of the concepts lie within $[0, 1]$. Thus, we used unipolar sigmoid function in this study and assume that $\lambda = 1$.

The initial values of the concepts in the input vector and the weighted arcs are set to specific values based on the expert's beliefs. Afterwards, the system is free to interact. This interaction continues until the model:

- Reaches equilibrium at a fixed point, with the output values, being decimals in the interval, stabilizing at fixed numerical values.
- Exhibits limit cycle behavior, with the output values falling in a loop of numerical values under a specific time period.
- Exhibits a chaotic behavior, with each output value reaching a variety of numerical values in a non-deterministic, random way.

Modeling a system using FCM has several advantages. FCMs are very simple, flexible and powerful tools for analyzing and modeling the real world as a collection of concepts and causal relationships. This simplicity helps the decision makers better understand the underlying formal model and its execution. In addition, they show an abstract representation and are capable of fuzzy reasoning (Stach, Kurgan, Pedrycz, & Reformat, 2005). Furthermore, even if the initial map of the problem is incomplete or incorrect, further additions to the map can be included, and the effects of new parameters can be quickly seen (Sharif & Irani, 2006). Therefore, FCM is chosen as a modeling approach in this study to simulate the system vulnerability behavior by taking into account the possible interrelationships among the system functions.

4. Fuzzy integrated vulnerability assessment model (FIVAM)

The proposed FIVAM framework in this study is based on fuzzy set theory, SMART and FCM methodology in the GDM environment. In this integrated utilization, fuzzy SMART is used as a simple and effective MCDM technique to weight the vulnerability criteria and to calculate the initial vulnerability value of the components with respect to these weighted criteria. After calculating the initial vulnerability values of all components, the physical dependencies of functions on components and the logical dependencies of system on functions are determined. Then, the initial vulnerability values of both the functions and the system are computed using these dependencies and component vulnerability values ignoring the possible interdependencies among the system functions. In the next phase, FCM methodology is applied to simulate the system vulnerability behavior depending on the vulnerabilities and the interdependencies among the system functions. After calculating the vulnerability values of the functions in the long run by using FCM, the system function and component vulnerabilities are recalculated by considering the effects of these possible interdependencies among the system functions. According to these results, the most critical functions and components in the system are determined and ranked. Finally, the vulnerabilities before and after the FCM simulation are compared and evaluated.

The proposed approach consists of the following steps is shown in Fig. 4.

Step 1: Form a working group. The group size influences the effectiveness of the GDM. As Yetton and Botter (1983) pointed out groups of five are the most effective and odd numbered groups help avoid decision deadlocks.

Assume that there is a group of s decision makers/experts (DMs) (D_i, $i = 1, 2, \ldots, s$) who are responsible for all the activities in the vulnerability assessment process.

Step 2: Characterize the system defended. The DMs organize series of meetings for identifying the system functions and system components considering the system mission and system boundaries. Then, a hierarchical system structure is constructed using this information.

Assume that there are t system functions (F_j, $j = 1, 2, \ldots, t$) and there are u_{F_j} system components (T_{jk}, $j = 1, 2, \ldots, t$, $k = 1, 2, \ldots, u_{F_j}$) that are required by function F_j to work properly.

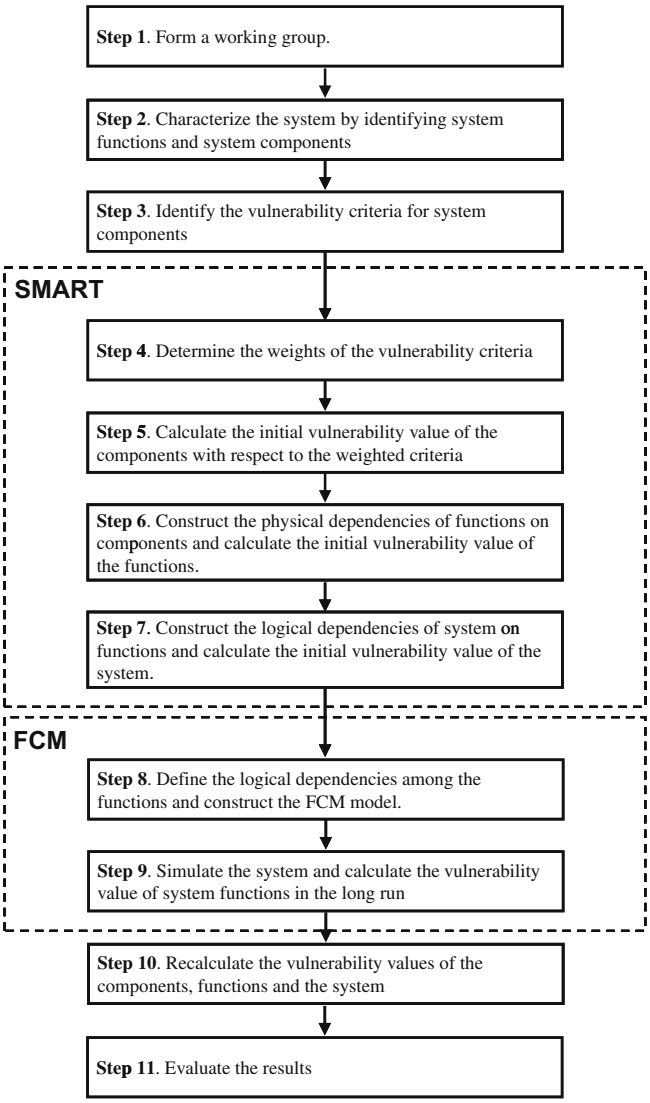

Fig. 4. The steps of FIVAM approach.

Step 3: Identify the vulnerability criteria for system components. The DMs use brainstorming GDM method for identifying the relevant criteria of the internal and external environment on vulnerability assessment of components. Then, these criteria are categorized as qualitative or quantitative, and quantitative criteria are also categorized as cost or benefit (polarity).

Let C_l, $l = 1, 2, \ldots, v$ be the vulnerability criteria.

Step 4: Determine the weights of the vulnerability criteria. Each DM assigns linguistic weighting variables shown in Table 1 for each criterion. Then, these fuzzy values are aggregated and the relative importance of the criteria is determined.

Let $\widetilde{W}_{il} = (a_{il}, b_{il}, c_{il}), i = 1, 2, \ldots, s, l = 1, 2, \ldots, v$ be the TFN corresponding to the linguistic variable given to criterion C_l by decision maker D_i. The aggregated fuzzy criterion weight, $\widetilde{W}_{C_l} = (a_{C_l}, b_{C_l}, c_{C_l}), l = 1, 2, \ldots, v$, of criterion C_l assessed by the group of s DMs is calculated as follows:

$$\widetilde{W}_{C_l} = \frac{1}{s} \otimes \sum_{i=1}^{s} \widetilde{W}_{il}, \tag{5}$$

where $a_{C_l} = \frac{1}{s} \otimes \sum_{i=1}^{s} a_{il}$, $b_{C_l} = \frac{1}{s} \otimes \sum_{i=1}^{s} b_{il}$ and $c_{C_l} = \frac{1}{s} \otimes \sum_{i=1}^{s} c_{il}$.

Then, the defuzzification of $\widetilde{W}_{C_l}$, denoted by $d(\widetilde{W}_{C_l})$ is calculated using Eq.(2) as follows:

$$d(\widetilde{W}_{C_l}) = \frac{1}{3}(a_{C_l} + b_{C_l} + c_{C_l}), \quad l = 1, 2, \ldots, v. \tag{6}$$

As the fuzzy SMART requires cardinal weights that are normalized to sum to 1, the crisp value of weight for criterion C_l, denoted as W_{C_l}, is given by

$$W_{C_l} = \frac{d(\widetilde{W}_{C_l})}{\sum_{l=1}^{v} d(\widetilde{W}_{C_l})}, \quad l = 1, 2, \ldots, v, \tag{7}$$

where $\sum_{l=1}^{v} W_{C_l} = 1$.

Step 5: Calculate the initial vulnerability value of the components with respect to the weighted criteria. The DMs use linguistic rating variables shown in Table 2 to assess fuzzy ratings of components with respect to vulnerability criteria, and then compute aggregated fuzzy ratings.

Let $\tilde{x}_{ijkl} = (a_{ijkl}, b_{ijkl}, c_{ijkl}),\ i = 1, 2, \ldots, s,\ j = 1, 2, \ldots, t,\ k = 1, 2, \ldots, u_{F_j},\ l = 1, 2, \ldots, v$ be the linguistic rating assigned to the component T_{jk} of function F_j for qualitative/subjective criterion C_l by decision maker D_i. Similarly, let $\tilde{q}_{ijkl} = (d_{ijkl}, e_{ijkl}, f_{ijkl}),\ i = 1, 2, \ldots, s,\ j = 1, 2, \ldots, t,\ k = 1, 2, \ldots, u_{F_j},\ l = 1, 2, \ldots, v$ be the TFN (or crisp) cost or benefit value assessed to the component T_{jk} of function F_j for quantitative/objective criterion C_l by decision maker D_i. The following equations are applied to normalize the quantitative value.

$$\tilde{x}_{ijkl} = \frac{\tilde{q}_{ijkl} - \min\limits_{jk}\{d_{ijkl}\}}{\max\limits_{jk}\{f_{ijkl}\} - \min\limits_{jk}\{d_{ijkl}\}} \otimes 10, \tag{8}$$

where $\tilde{x}_{ijkl}$ denotes the normalized fuzzy rating of fuzzy benefit $\tilde{q}_{ijkl}$.

$$\tilde{x}_{ijkl} = \frac{\max\limits_{jk}\{f_{ijkl}\} - \tilde{q}_{ijkl}}{\max\limits_{jk}\{f_{ijkl}\} - \min\limits_{jk}\{d_{ijkl}\}} \otimes 10, \tag{9}$$

where $\tilde{x}_{ijkl}$ denotes the normalized fuzzy rating of fuzzy cost $\tilde{q}_{ijkl}$.

The aggregated fuzzy rating, $\tilde{x}_{jkl} = (a_{jkl}, b_{jkl}, c_{jkl}),\ j = 1, 2, \ldots, t,\ k = 1, 2, \ldots, u_{F_j},\ l = 1, 2, \ldots, v$, of component T_{jk} for criterion C_l is calculated as

$$\tilde{x}_{jkl} = \frac{1}{s} \otimes \sum_{i=1}^{s} \tilde{x}_{ijkl}. \tag{10}$$

Then, the initial fuzzy vulnerability value of component k of function j, $\widetilde{V}_{T_{jk}}$, can be obtained by:

$$\widetilde{V}_{T_{jk}} = \sum_{l=1}^{v} W_{C_l} \otimes \tilde{x}_{jkl}, \quad j = 1, 2, \ldots, t,\ k = 1, 2, \ldots, u_{F_j}, \tag{11}$$

where $\widetilde{V}_{T_{jk}} = (a_{jk}, b_{jk}, c_{jk}),\ j = 1, 2, \ldots, t,\ k = 1, 2, \ldots, u_{F_j}$.

The component vulnerability value $\widetilde{V}_{T_{jk}}$ is defuzzified using Eq. (2) and component vulnerability value $d(\widetilde{V}_{T_{jk}})$ is determined. Then, normalized crisp component vulnerability value $V_{T_{jk}}$ is calculated as follows:

$$V_{T_{jk}} = \frac{d(\widetilde{V}_{T_{jk}})}{\max\limits_{jk}(d(\widetilde{V}_{T_{jk}}))}, \quad j = 1, 2, \ldots, t,\ k = 1, 2, \ldots, u_{F_j}. \tag{12}$$

Step 6: Construct the physical dependencies of functions on components and calculate the initial vulnerability value of the functions. To determine the initial function vulnerabilities that depend on component vulnerability values, the DMs assign linguistic variables shown in Table 1 for the degree of dependency between function and component.

Let $\widetilde{W}_{ijk} = (a_{ijk}, b_{ijk}, c_{ijk}),\ i = 1, 2, \ldots, s,\ j = 1, 2, \ldots, t,\ k = 1, 2, \ldots, u_{F_j}$ be the TFN corresponding to the linguistic variable given to the dependency degree of function F_j on component T_{jk} by decision maker D_i. The aggregated fuzzy dependency degree, $\widetilde{W}_{T_{jk}} = (a_{T_{jk}}, b_{T_{jk}}, c_{T_{jk}}),\ j = 1, 2, \ldots, t,\ k = 1, 2, \ldots, u_{F_j}$ of component T_{jk} assessed by the group of s DMs is determined as:

$$\widetilde{W}_{T_{jk}} = \frac{1}{s} \otimes \sum_{i=1}^{s} \widetilde{W}_{ijk}. \tag{13}$$

Then, the defuzzified dependency degree, $d(\widetilde{W}_{T_{jk}})$, is calculated using Eq. (2) and normalized as follows:

$$W_{T_{jk}} = \frac{d(\widetilde{W}_{T_{jk}})}{\sum_{k=1}^{u_{F_j}} d(\widetilde{W}_{T_{jk}})}, \quad j = 1, 2, \ldots, t \tag{14}$$

where $\sum_{k=1}^{u_{F_j}} W_{T_{jk}} = 1,\ j = 1, 2, \ldots, t$.

The initial fuzzy vulnerability value for function F_j, denoted as $\widetilde{V}_{F_j}$, is the sum product of all component vulnerability values and their associated dependency degree as follows:

$$\widetilde{V}_{F_j} = \sum_{k=1}^{u_{F_j}} (W_{T_{jk}} \otimes \widetilde{V}_{T_{jk}}), \quad j = 1, 2, \ldots, t, \tag{15}$$

where $\widetilde{V}_{F_j} = (a_j, b_j, c_j),\ j = 1, 2, \ldots, t$.

Since, the threshold function in FCM model requires crisp concept values within [0, 1], normalized crisp function vulnerability value V_{F_j} is calculated as follows:

$$V_{F_j} = \frac{d(\widetilde{V}_{F_j})}{\max\limits_{j}(d(\widetilde{V}_{F_j}))}, \quad j = 1, 2, \ldots, t, \tag{16}$$

where $d(\widetilde{V}_{F_j})$ is the defuzzified function vulnerability value.

Step 7: Construct the logical dependencies of system on functions and calculate the initial vulnerability value of the system. To determine the system vulnerability that depends on function vulnerability values, the DMs assign linguistic variables shown in Table 1 for the degree of dependency between system and function.

Let $\widetilde{W}_{ij} = (a_{ij}, b_{ij}, c_{ij}),\ i = 1, 2, \ldots, s,\ j = 1, 2, \ldots, t$ be the TFN corresponding to the linguistic variable given to the dependency degree of system on function F_j by decision maker D_i. The aggregated fuzzy dependency degree, $\widetilde{W}_{F_j} = (a_{F_j}, b_{F_j}, c_{F_j}),\ j = 1, 2, \ldots, t$ of component F_j assessed by the group of s DMs is defined as:

$$\widetilde{W}_{F_j} = \frac{1}{s} \otimes \sum_{i=1}^{s} \widetilde{W}_{ij}. \tag{17}$$

As in the previous steps, the fuzzy dependency degree, $\widetilde{W}_{F_j}$, is defuzzified and normalized value, W_{F_j}, is calculated. Then, the

vulnerability value for the system S, denoted as V_S, is the sum product of all function vulnerability values and their associated dependency degree as follows:

$$V_S = \sum_{j=1}^{t} (W_{F_j} \otimes V_{F_j}). \quad (18)$$

Step 8: Define the logical dependencies among the functions and construct the FCM model. The DMs use linguistic influence variables shown in Table 3 to assess fuzzy causal relationships (influences) among the system functions.

Let $\tilde{r}_{ijm} = (a_{ijm}, b_{ijm}, c_{ijm})$, $i = 1,2,\ldots,s$, $j,m = 1,2,\ldots,t$ be the TFN corresponding to the linguistic variable assigned to the influence degree of function F_j to function F_m by decision maker D_i. The aggregated fuzzy influence value, $\tilde{r}_{jm} = (a_{jm}, b_{jm}, c_{jm})$, $j, m = 1,2,\ldots,t$ where $\tilde{r}_{jj} = 0$, is calculated as:

$$\tilde{r}_{jm} = \frac{1}{s} \otimes \sum_{i=1}^{s} \tilde{r}_{ijm}. \quad (19)$$

As the unipolar sigmoid function in FCM model requires crisp values, the crisp influence value r_{jm} is determined by defuzzifying the aggregated fuzzy influence value $\tilde{r}_{jm}$ using Eq. (2).

Step 9: Simulate the system and calculate the vulnerability value of the system functions in the long run. The vulnerability value of a system function in each iteration is calculated using Eq. (4) as follows:

$$V_{F_j}^{z+1} = f\left(V_{F_j}^{z} + \sum_{m=1, m\neq j}^{t} r_{mj} V_{F_m}^{z}\right), \quad j = 1,2,\ldots,t. \quad (20)$$

When the model reaches equilibrium at a fixed point after some iterations, new crisp vulnerability value of for function F_j, denoted as $V_{F_j}^{e}$, is determined.

Step 10: Recalculate the vulnerability values of the components, functions and the system. As the result of the FCM simulation is the function vulnerabilities at the equilibrium point, first of all, the hidden vulnerability of the functions have to be determined. If function F_j influences function F_m, there is a hidden vulnerability on cause function F_j because of the dependency of F_m on F_j. This hidden vulnerability $V_{F_j}^{h}$ of a function F_j is calculated as

$$V_{F_j}^{h} = \sum_{m=1, m\neq j}^{t} (r_{jm} \times V_{F_m}^{e}), \quad j = 1,2,\ldots,t. \quad (21)$$

Then, the real vulnerability value of function F_j is the sum of initial and the hidden vulnerabilities as follows:

$$V'_{F_j} = V_{F_j} + V_{F_j}^{h}, \quad j = 1,2,\ldots,t. \quad (22)$$

The hidden vulnerability value of the system, V_S^h, is calculated by the sum product of hidden function vulnerability values and their associated dependency degree as

$$V_S^h = \sum_{j=1}^{t} (W_{F_j} \times V_{F_j}^{h}). \quad (23)$$

The real vulnerability value of the system, V'_S, is therefore given by

$$V'_S = V_S + V_S^h. \quad (24)$$

Similarly, the hidden function vulnerabilities calculated by the FCM simulation have to be reflected to the component vulnerabilities proportional to the component-function dependencies. To do this, the vulnerability values of the components are recalculated by the following equations:

$$V_{T_{jk}}^{h} = W_{T_{jk}} \times V_{F_j}^{h}, \quad j = 1,2,\ldots,t, \ k = 1,2,\ldots,u_{F_j}, \quad (25)$$

$$V'_{T_{jk}} = V_{T_{jk}} + V_{T_{jk}}^{h}, \quad j = 1,2,\ldots,t, \ k = 1,2,\ldots,u_{F_j}. \quad (26)$$

Step 11: Evaluate the results. The system components and functions based on their vulnerability values before and after FCM simulation are ranked and compared. Furthermore, the hidden vulnerabilities are presented and discussed.

The detailed descriptions of each step are elaborated in the following illustrative case study section.

5. An illustrative example

In this section, the proposed FIVAM approach as described in Section 4 is applied to a hypothetical Airport X to discover hidden vulnerabilities for improving its site security. Modern airports with their runways, taxiways, aprons, passenger terminals, ground handling and flight navigation equipment are very complex facilities Ashford et al., 1997. Simply, the mission of an airport is to land, to unload payload, to load payload and to take off aircrafts. When the security requirements are considered against the possible terrorist attacks, the challenge of vulnerability assessment for an airport becomes very complicated. Therefore, it is thought that an airport case can be an interesting example.

Note that all the values used throughout this example are purely generic and notional. Even though this case study is very simple and the results may not increase our knowledge about

Table 4
Hierarchical system structure of Airport X.

Components		Functions		System
T_{11}	Airfield maintenance building	F_1	Ground Handling Service (GHS)	Airport X (S)
T_{12}	Fuel complex building			
T_{21}	Passenger terminal	F_2	Passenger Service (PS)	
T_{22}	Parking facility			
T_{23}	Bus station			
T_{31}	Custom building	F_3	Cargo & Baggage Service (CBS)	
T_{32}	Cargo terminal			
T_{41}	Air traffic control & tower	F_4	Air Traffic Management Service (ATMS)	
T_{42}	Apron			
T_{43}	Runway & taxiway			
T_{51}	Main entrance & security control building	F_5	Emergency Service (ES)	
T_{52}	Security building			
T_{53}	Aircraft rescue and fire fighting building			
T_{54}	Police station building			
T_{55}	Fuel complex guard building			
T_{56}	Guard tower			
T_{57}	Fencing			
T_{61}	Heating center building	F_6	Infrastructure Service (IS)	
T_{62}	Power center building			
T_{63}	Water storage building			

the system, it validates the FIVAM approach. A step-by-step algorithm for this example is as follows:

Step 1: In this case study, the number of DMs who were involved in the decision-making process is selected as five. In order to extend the assessment to account for the conflicts among different interest groups who have different objectives, goals and criteria; one terrorism expert, one security expert, two representatives from the airport administration and one academician from the Faculty of Aeronautics have participated in the decision process as DMs.

In the evaluation process, while the terrorism and security experts mostly deal with the security issues, representatives from an airport administration and the academician concern the functionality of Airport X. The authors support these DMs with their technical knowledge on the methodology.

Series of meetings were organized with participation of these DMs and all the issues including comments and suggestions are discussed at these meetings.

Step 2: The DMs identified the relevant functions and components of Airport X by considering the following three questions: "What is the principal mission of Airport X?", "What system functions are essential to carry out this mission by Airport X?" and "What system components do these system functions depend on for their success?". For simplification, only the critical functions have been considered and their most relevant components have been focused on at the component abstraction level in this study.

In order to accomplish its mission, the DMs determined that Airport X has to provide six main functions: (1) Ground handling service (GHS) for servicing, maintenance and engineering of aircrafts; (2) Passenger service (PS) for gate-management, check-in

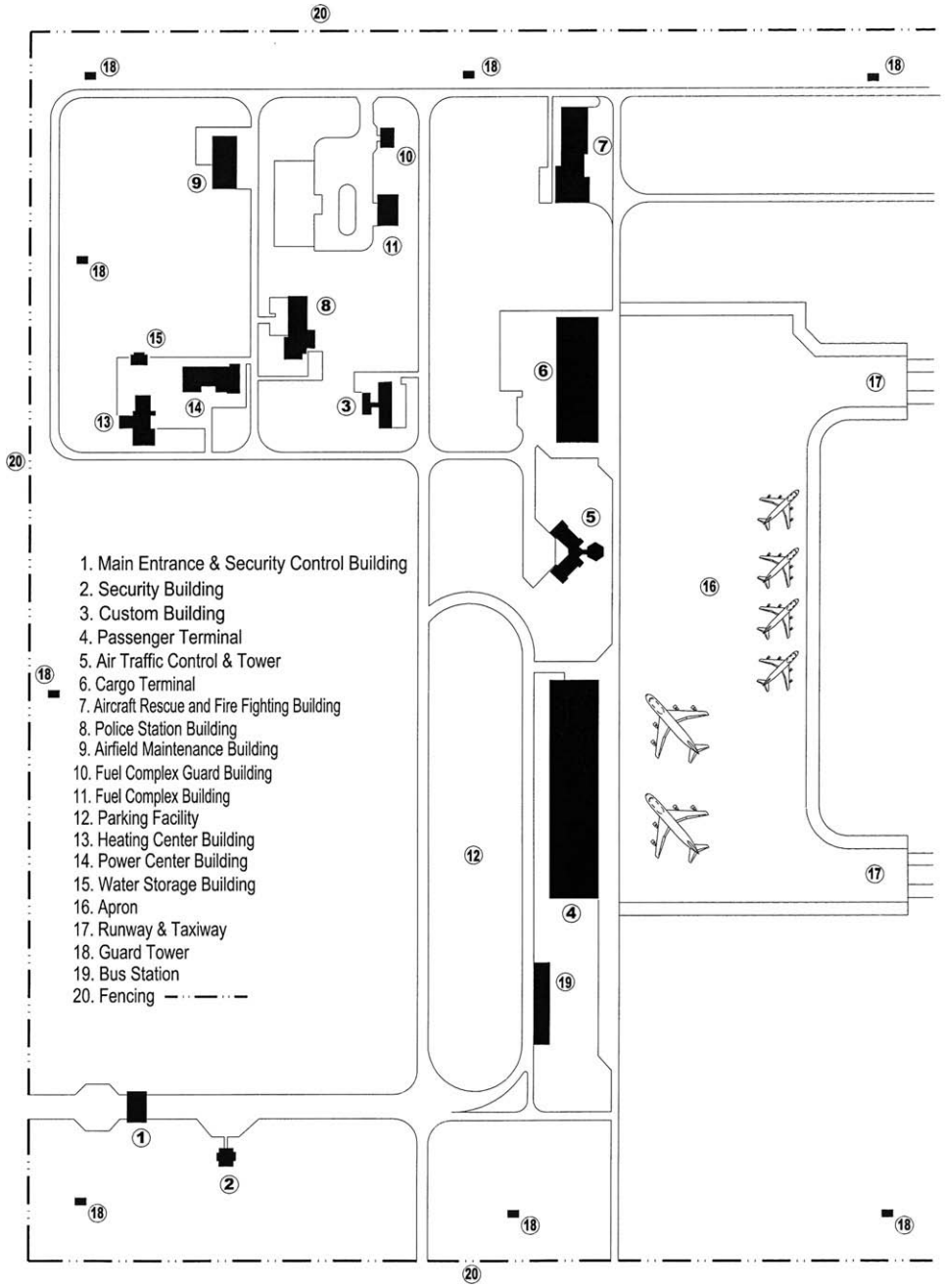

Fig. 5. Sketch of Airport X.

desk allocation, and flight-information displays; (3) Cargo and baggage service (CBS) function for transportation of payload; (4) Air traffic management service (ATMS) for approach, landing, taxiing, take off and departure of aircrafts; (5) Emergency services (ES) for fire fighting, medical and security services; and (6) Infrastructure services (IS) for maintaining the general service capability of the airport.

After identifying the relevant functions of Airport X, the DMs determined 20 system components by answering the third question mentioned above. Table 4 summarizes the functions and the components of Airport X in a hierarchical structure and Fig. 5 illustrates the sketch of Airport X.

Step 3: In this study, the key factors for assessing the vulnerability of Airport X are derived from literature reviews, comprehensive investigation and consultation with DMs. After a comprehensive discussion, all the evaluation criteria for the component vulnerability assessment are identified accordingly. The five DMs collectively set up five criteria and the detail descriptions of these criteria are listed below:

- Deterrence (C_1): Deterrence is defined as defense methods implemented that are perceived by terrorists as too difficult to defeat. The presence of security controls such as access control, perimeter protection, proper lighting and use of metal detector/X-ray/Closed Circuit Television at entrance and at all critical locations increase the deterrence of the component by lowering the attractiveness of a component as a target.
- Detection (C_2): Detection is defined as the capability of determining that an unauthorized terrorist action has occurred or is occurring, including: sensing, communicating alarm to control center, and assessing the alarm (Ezell, 2007). The high value of detection decreases the vulnerability of a component.
- Delay (C_3): Delay is defined as the time that an element of a physical protection system is designed to impede terrorist penetration into or exit from the protected area (Ezell, 2007). Decreasing the delay will reduce the potential for a component to be a target.
- Response (C_4): Response is defined as a time to respond to a threat. Response activities occurred immediately after a terrorist attack includes stabilizing affected areas, immediate medical care and evacuation during the terrorist attack. Short response time decreases the vulnerability of a component.
- Recovery (C_5): Recovery is defined as a time to return the affected areas and persons to their pre-event status. It includes restoring critical elements, assisting affected persons, and coordinating relief efforts after the possible terrorist attacks for the worst case scenario. Quicker recovery of a component from an attack indicates that the component is less vulnerable.

As a result, Deterrence (C_1) and Detection (C_2) are the qualitative criteria; whereas Delay (C_3), Response (C_4) and Recovery (C_5) are the quantitative benefit criteria.

Step 4: The linguistic weighting variables (Table 1) and their respective fuzzy numbers for DMs are then used to assess the importance weights of the evaluation criteria. These assigned fuzzy values are aggregated by arithmetic mean method using Eq. (5) and the fuzzy weights of individual criteria can then be determined (Table 5). Furthermore, crisp and normalized weight values

Table 5
The relative importance weights of the five criteria by five DMs.

Criteria	Polarity	DM's linguistics weights					Aggregated weights		
		DM_1	DM_2	DM_3	DM_4	DM_5	Fuzzy number	Defuzzified	Normalized
C_1	–	H	H	VH	MH	M	(0.62, 0.8, 0.92)	0.780	0.275
C_2	–	H	MH	M	M	ML	(0.38, 0.58, 0.76)	0.573	0.202
C_3	+	M	ML	L	M	ML	(0.16, 0.34, 0.54)	0.347	0.122
C_4	+	MH	M	H	M	MH	(0.46, 0.66, 0.84)	0.653	0.231
C_5	+	M	VL	H	M	M	(0.32, 0.48, 0.64)	0.480	0.169

Polarity: '+' = benefit criteria, '–' = cost criteria.

Table 6
Aggregated fuzzy ratings and vulnerability of components.

	Aggregated fuzzy ratings regarding each criterion					Component vulnerability value			
	C_1	C_2	C_3	C_4	C_5	Fuzzy number	Defuz.	Norm.	Rank
T_{11}	(2.6, 4.6, 6.6)	(1.8, 3.2, 5)	(4.6, 6.6, 8.4)	(5, 7, 8.6)	(4.6, 6.6, 8.4)	(3.58, 5.45, 7.26)	5.430	0.904	5
T_{12}	(3, 5, 7)	(3.2, 5, 7)	(3.4, 5.4, 7.4)	(3.8, 5.8, 7.8)	(4.2, 6.2, 8.2)	(3.48, 5.44, 7.44)	5.450	0.907	4
T_{21}	(4.6, 6.6, 8.4)	(0.2, 1.2, 3)	(0.2, 1.2, 3)	(2, 3.8, 5.8)	(6.6, 8.4, 9.6)	(2.91, 4.51, 6.25)	4.556	0.758	9
T_{22}	(1, 2.6, 4.6)	(5.8, 7.6, 8.8)	(3, 5, 7)	(2.2, 4.2, 6.2)	(0.2, 1.2, 3)	(2.36, 4.04, 5.84)	4.079	0.679	11
T_{23}	(0.8, 2.6, 4.6)	(5, 7, 8.6)	(4.6, 6.6, 8.4)	(3.4, 5.4, 7.4)	(0.2, 1.2, 3)	(2.61, 4.39, 6.25)	4.417	0.735	10
T_{31}	(3, 5, 7)	(4.2, 6.2, 8.2)	(4.2, 6.2, 8)	(1.8, 3.8, 5.8)	(1, 2.4, 4.2)	(2.77, 4.67, 6.61)	4.687	0.780	8
T_{32}	(2.6, 4.6, 6.6)	(5, 7, 8.8)	(5, 7, 8.8)	(4.2, 6.2, 8.2)	(0.8, 2, 3.8)	(3.44, 5.31, 7.21)	5.320	0.886	6
T_{41}	(3.8, 5.8, 7.6)	(0.4, 1.8, 3.8)	(0.4, 1.6, 3.4)	(2.6, 4.6, 6.6)	(7.4, 9, 9.8)	(3.03, 4.74, 6.46)	4.744	0.790	7
T_{42}	(1, 2.6, 4.6)	(5.4, 7.4, 9)	(1.2, 3, 5)	(2.6, 4.6, 6.6)	(0, 0.4, 1.8)	(2.11, 3.71, 5.53)	3.783	0.630	12
T_{43}	(1, 2.6, 4.6)	(3.4, 5.4, 7.4)	(2.2, 4.2, 6.2)	(3, 5, 7)	(0.2, 1.2, 3)	(1.96, 3.68, 5.64)	3.760	0.626	13
T_{51}	(0, 0.4, 1.8)	(0, 0.2, 1.4)	(0, 0.2, 1.4)	(0, 0.4, 1.8)	(0.8, 2.2, 4.2)	(0.14, 0.64, 2.08)	0.951	0.158	20
T_{52}	(0, 0.2, 1.4)	(0, 0.2, 1.4)	(0, 0, 1)	(0, 0.2, 1.4)	(1.8, 3.8, 5.8)	(0.3, 0.79, 2.1)	1.062	0.177	19
T_{53}	(1.6, 3.4, 5.4)	(0.6, 2.2, 4.2)	(0.2, 1, 2.6)	(1.2, 3, 5)	(1, 2.6, 4.6)	(1.03, 2.64, 4.59)	2.752	0.458	14
T_{54}	(0, 0.2, 1.4)	(0, 0.4, 1.8)	(0, 0.2, 1.4)	(0.2, 1, 2.6)	(2.6, 4.6, 6.6)	(0.49, 1.17, 2.64)	1.432	0.238	16
T_{55}	(0, 0.6, 2.2)	(0.4, 1.8, 3.8)	(0.4, 1.4, 3)	(0, 0.6, 2.2)	(0.2, 1.2, 3)	(0.16, 1.04, 2.76)	1.321	0.220	17
T_{56}	(0, 0.6, 2.2)	(0.4, 1.8, 3.8)	(0.2, 1.2, 3)	(0, 0.6, 2.2)	(0, 0.4, 1.8)	(0.11, 0.88, 2.55)	1.181	0.197	18
T_{57}	(0, 0.6, 2.2)	(0.2, 1.2, 3)	(3.8, 5.8, 7.8)	(0.2, 1.4, 3.4)	(0, 0.2, 1.4)	(0.55, 1.47, 3.19)	1.738	0.289	15
T_{61}	(3, 5, 7)	(3.8, 5.8, 7.6)	(2.6, 4.6, 6.6)	(2.6, 4.6, 6.6)	(7, 8.8, 9.8)	(3.7, 5.66, 7.45)	5.606	0.933	2
T_{62}	(3.8, 5.8, 7.8)	(3, 5, 7)	(3.8, 5.8, 7.8)	(3, 5, 7)	(7.8, 9.4, 10)	(4.13, 6.06, 7.83)	6.007	1.000	1
T_{63}	(2.6, 4.6, 6.6)	(3.4, 5.4, 7.4)	(3.4, 5.4, 7.4)	(2.6, 4.6, 6.6)	(7.4, 9, 9.8)	(3.67, 5.61, 7.4)	5.560	0.926	3

are also calculated by using Eqs. (6) and (7) and included in the table.

The weights of the criteria presented in Table 5 reveal that the most important criteria for assessing vulnerability of a component is "deterrence" ($W_{C_1} = 0.275$); whereas the least important criteria is "delay" ($W_{C_3} = 0.122$).

Step 5: The linguistic rating variables (Table 2) and their respective fuzzy numbers for DMs are used to assess the fuzzy ratings of the 20 components with respect to each qualitative/quantitative criterion. As the DMs sometimes have different understandings of the same performance data, the DMs adopted linguistic terms in Table 2 to express their opinions about the rating of every component regarding each quantitative criterion, Delay (C_3), Response (C_4), and Recovery (C_5) in this case study. For instance, some DMs might think that 3 minutes was a "good" or "very good" delay for "Air Traffic Control & Tower" component, while the others might think that value was "fair" or "medium poor". Alternatively, in accordance with crisp data, the normalized values of individual quantitative criteria can be computed by using Eq. (8) or Eq. (9). The aggregated fuzzy rating of each criterion can be computed by Eq. (10), and then, the aggregated fuzzy ratings are formed. The fuzzy vulnerability values of components are obtained using Eq. (11) and the results are listed in Table 6. Furthermore, crisp and normalized vulnerability values of components and their rankings are also calculated by using Eq. (12) and included in the table.

In Table 6, it is identified that the three most vulnerable components are "Power Center Building" ($V_{T_{62}} = 1.000$), "Heating Center Building" ($V_{T_{61}} = 0.933$) and "Water Storage Building" ($V_{T_{63}} = 0.926$); whereas the three least vulnerable components are "Main Entrance & Security Control Building" ($V_{T_{51}} = 0.158$), "Security Building" ($V_{T_{52}} = 0.177$) and "Guard Tower" ($V_{T_{56}} = 0.197$). These are the most and the least probable possible targets for the terrorist attacks.

Step 6: In this step, the DMs use the linguistic weighting variables in Table 1 to assess the physical degree of dependency between functions and components. These assigned fuzzy values are aggregated and defuzzified using Eqs. (13) and (14) and the crisp dependency degrees (weights) are determined (Table 7). The fuzzy vulnerability values of functions are then calculated by the sum product of all component vulnerability values and their associated dependency degrees using Eq. (15) (Table 7). In addition to this, crisp and normalized vulnerability values of functions and their rankings are also computed using Eq. (16) and included in the table.

In Table 7, it is seen that the most vulnerable function is "Infrastructure Service (IS)" ($V_{F_6} = 1.000$). On the other hand, the least vulnerable function is "Emergency Service (ES)" ($V_{F_5} = 0.245$).

Step 7: The DMs assign the linguistic weighting variables in Table 1 for the logical degree of dependency between Airport X and its functions. These assigned fuzzy values are aggregated using Eq. (17). The crisp vulnerability value of Airport X is then calculated by the sum product of all function vulnerability values and their associated aggregated dependency degrees using Eq. (18) (Table 8). As seen from the table, the Airport X has a vulnerability value of 0.749. By the end of this step, vulnerability assessment is conducted using the SMART approach like the other classical models. However, in the next steps FCM is applied to identify and determine the real and hidden vulnerabilities caused by the functional interdependencies among the system functions.

Step 8: The linguistic influence variables (Table 3) and their respective fuzzy numbers for DMs are then used to define the causal relationships among the functions of Airport X. These fuzzy values are aggregated by using Eq. (19) and crisp influence matrix is constructed after defuzzication for the FCM simulation (Table 9). Furthermore, the FCM model for the functions of Airport X is presented in Fig. 6.

Step 9: The FCM model is simulated using Eq. (20) and function vulnerability values reach an equilibrium state after a few itera-

Table 8
Dependency degree of functions and vulnerability of Airport X.

Func.	Aggregated degree of dependency			System vulnerability value
	Fuzzy number	Defuzzified	Normalized	
F_1	(0.42, 0.62, 0.82)	0.62	0.15	0.749
F_2	(0.7, 0.88, 0.98)	0.85	0.21	
F_3	(0.34, 0.54, 0.74)	0.54	0.13	
F_4	(0.74, 0.9, 0.98)	0.87	0.22	
F_5	(0.42, 0.62, 0.8)	0.61	0.15	
F_6	(0.34, 0.54, 0.74)	0.54	0.13	

Table 7
Dependency degree of components and vulnerability of functions.

Func.	Comp.	Aggregated degree of dependency			Function vulnerability value			
		Fuzzy number	Defuzzified	Normalized	Fuzzy number	Defuzzified	Normalized	Rank
F_1	T_{11}	(0.66, 0.84, 0.96)	0.82	0.52	(3.53, 5.45, 7.35)	5.440	0.932	2
	T_{12}	(0.58, 0.78, 0.92)	0.76	0.48				
F_2	T_{21}	(0.82, 0.96, 1)	0.93	0.73	(2.79, 4.42, 6.19)	4.470	0.766	4
	T_{22}	(0.04, 0.16, 0.34)	0.18	0.14				
	T_{23}	(0.04, 0.14, 0.3)	0.16	0.13				
F_3	T_{31}	(0.38, 0.58, 0.78)	0.58	0.42	(3.16, 5.04, 6.96)	5.051	0.865	3
	T_{32}	(0.62, 0.8, 0.94)	0.79	0.58				
F_4	T_{41}	(0.82, 0.96, 1)	0.93	0.50	(2.52, 4.22, 6.03)	4.256	0.729	5
	T_{42}	(0.16, 0.34, 0.54)	0.35	0.19				
	T_{43}	(0.38, 0.58, 0.78)	0.58	0.31				
F_5	T_{51}	(0.46, 0.66, 0.84)	0.65	0.21	(0.38, 1.17, 2.74)	1.429	0.245	6
	T_{52}	(0.38, 0.58, 0.76)	0.57	0.19				
	T_{53}	(0.26, 0.46, 0.66)	0.46	0.15				
	T_{54}	(0.26, 0.46, 0.66)	0.46	0.15				
	T_{55}	(0.1, 0.26, 0.46)	0.27	0.09				
	T_{56}	(0.26, 0.46, 0.66)	0.46	0.15				
	T_{57}	(0.04, 0.16, 0.34)	0.18	0.06				
F_6	T_{61}	(0.1, 0.24, 0.42)	0.25	0.19	(3.95, 5.89, 7.67)	5.838	1.000	1
	T_{62}	(0.62, 0.82, 0.96)	0.80	0.60				
	T_{63}	(0.1, 0.26, 0.46)	0.27	0.21				

Table 9
Causal relationships among the functions of Airport X.

Functions	F_1	F_2	F_3	F_4	F_5	F_6
F_1	0.00	0.36	0.00	0.27	0.00	0.00
F_2	0.00	0.00	0.00	0.25	0.00	0.00
F_3	0.00	0.27	0.00	0.00	0.00	0.00
F_4	0.00	0.64	0.00	0.00	0.00	0.00
F_5	0.67	0.44	0.35	0.59	0.00	0.64
F_6	0.56	0.38	0.27	0.38	0.50	0.00

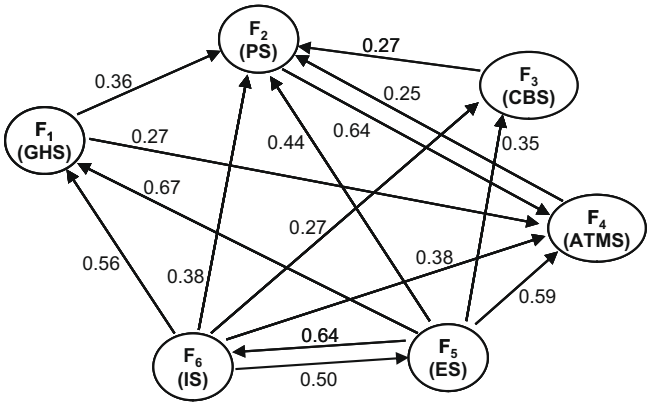

Fig. 6. FCM model for Airport X.

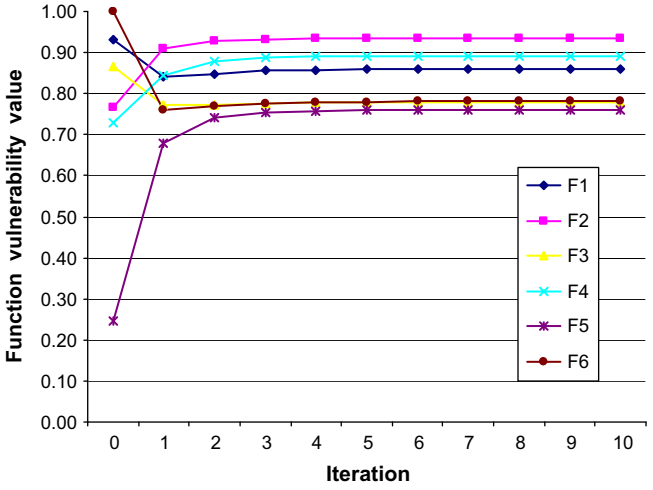

Fig. 7. Equilibrium state of the function vulnerability values.

tions. The calculated function vulnerability values for 10 iterations are presented in Table 10 and equilibrium of concept values are shown in Fig. 7.

As seen from Table 10 and Fig. 7, after the FCM simulation, PS function has become the most vulnerable function in the long run with a vulnerability value of $V_{F_2} = 0.935$. The reason is that, this function is affected by all the other functions. This means an increase in the vulnerability value of any function creates an increase in the vulnerability value of PS function. On the other hand, ES function has become relatively the least vulnerable function with $V_{F_5} = 0.759$ after the simulation as it is the least affected function in the system. The results in Table 10 also show that after the FCM simulation the most influenced function has the highest vulnerability value; whereas the least influenced function has the lowest vulnerability value.

Step 10: The hidden and real vulnerability values of the components, functions and the system are calculated using Eqs. (21)–(26) and shown in Table 11.

Step 11: The rankings and the vulnerability values before and after FCM simulation are presented in Table 11. It is observed that the ranks of functions and components are different due to the hidden vulnerabilities caused by the logical interdependencies among the functions. For instance, while IS function has the same rank before and after the simulation, ES functions has greatly different ranks. Although, this function has the least vulnerability before simulation, it becomes the second most vulnerable after simulation as it has the highest hidden vulnerability ($V^h_{F_5} = 2.293$). On the other hand, PS function becomes the least critical function of Airport X having the least real vulnerability value after simulation. It can be concluded that the IS function, with the real vulnerability of $V_{F_6} = 2.774$, is determined as the most critical function for Airport X.

At the component level, this rank difference is not as much as it is at the functional level. From Table 11, it is identified that "Power Center Building" having the highest real vulnerability of $V_{T_{62}} = 2.069$, is the most critical component for Airport X. This component also has the highest hidden vulnerability ($V^h_{T_{62}} = 1.069$). "Main Entrance & Security Control Building" has the least vulnerability ($V_{T_{51}} = 0.158$) and rank before the simulation, but its rank and criticality is increased by five after the simulation since it has the second highest hidden vulnerability ($V^h_{T_{51}} = 0.490$).

The high vulnerable or in other words most critical components of Airport X are the most probable possible targets for the terrorist attacks. Hence, the appropriate defense resource should be allocated in the following defense resource planning process to improve site security of Airport X.

Finally, the systematic application of the FIVAM satisfactorily contributes the overall vulnerability assessment process of Airport X. This approach can originally be utilized as a decision aid by the related managers; moreover, it provides both motivation and contributions on vulnerability assessment process as one of the critical administrative issue consistently.

Table 10
The vulnerability values of functions for 10 iterations.

Functions	Iterations									
	1	2	3	4	5	6	7	8	9	10
F_1	0.932	0.840	0.848	0.855	0.858	0.859	0.859	0.859	0.859	0.859
F_2	0.766	0.908	0.928	0.933	0.934	0.935	0.935	0.935	0.935	0.935
F_3	0.865	0.773	0.772	0.776	0.778	0.779	0.779	0.779	0.779	0.779
F_4	0.729	0.845	0.879	0.888	0.890	0.890	0.891	0.891	0.891	0.891
F_5	0.245	0.678	0.742	0.755	0.758	0.759	0.759	0.759	0.759	0.759
F_6	1.000	0.761	0.768	0.777	0.779	0.780	0.781	0.781	0.781	0.781

Table 11
Comparison of the vulnerability values.

	Before FCM simulation		After FCM simulation		Hidden vulnerability
	Vulnerability	Rank	Vulnerability	Rank	
System	0.749	–	1.621	–	0.872
Functions					
F_1	0.932	2	1.506	3	0.574
F_2	0.766	4	0.985	6	0.220
F_3	0.865	3	1.121	5	0.256
F_4	0.729	5	1.330	4	0.601
F_5	0.245	6	2.538	2	2.293
F_6	1.000	1	2.774	1	1.774
Components					
T_{11}	0.904	5	1.202	4	0.298
T_{12}	0.907	4	1.183	5	0.276
T_{21}	0.758	9	0.919	8	0.161
T_{22}	0.679	11	0.710	14	0.031
T_{23}	0.735	10	0.763	12	0.028
T_{31}	0.780	8	0.889	9	0.108
T_{32}	0.886	6	1.033	7	0.147
T_{41}	0.790	7	1.090	6	0.301
T_{42}	0.630	12	0.742	13	0.112
T_{43}	0.626	13	0.814	10	0.188
T_{51}	0.158	20	0.648	15	0.490
T_{52}	0.177	19	0.606	16	0.430
T_{53}	0.458	14	0.803	11	0.345
T_{54}	0.238	16	0.583	17	0.345
T_{55}	0.220	17	0.425	19	0.205
T_{56}	0.197	18	0.541	18	0.345
T_{57}	0.289	15	0.424	20	0.135
T_{61}	0.933	2	1.272	3	0.339
T_{62}	1.000	1	2.069	1	1.069
T_{63}	0.926	3	1.291	2	0.365

6. Conclusions

In the last decade, the number of terrorist attacks to the critical facilities has increased dramatically and combating the terrorism has gained more importance. Managing the risk of these facilities for the terrorist attacks depends on systematic and quantitative vulnerability assessment.

Vulnerability assessment should be conducted at three levels: system level, system function level and system component level. Furthermore, the most critical functions and components in the system have to be determined and ranked to support the following defense resource planning process.

When the nature of this problem is analyzed, it seems that the fuzzy SMART and FCM integration, proposed FIVAM framework, can be recognized as a suitable research methodology towards the solution of this problem. FIVAM takes the advantages of the fuzzy SMART for determining the vulnerability of system under multiple qualitative/quantitative criteria in GDM environment, and FCM for modeling the behavior of the system to monitor the vulnerability.

The case application of an example airport illustrates the utility and effectiveness of the proposed FIVAM framework. The quantitative findings on the case study highlight that possible interrelationships among the system functions are very significant in vulnerability assessment of a critical facility and they have to be taken into account in the system perspective. By doing this, hidden vulnerabilities can be identified consistently. That is why; the FIVAM framework becomes more realistic and applicable to overcome this issue. Furthermore, FIVAM can be utilized as a simple and practical toolkit for this type of real life problems for enhancing the current procedures in vulnerability assessment process. To realize this idea, FIVAM can be applied similarly in some cases to assess the vulnerability of any other facilities that can be a metro station, shopping mall, metro station, harbor, governmental facility, military bases, chemical plants, oil refinery, etc. In addition to this, both the number of evaluation criteria and system components can be increased in order to conduct a detailed assessment at the operational and tactical level.

The further research can be performed on extending the FIVAM framework to assign defense resources for the most vulnerable components to comprehensively support this critical decision-making problem. For this purpose, SWOT analysis as a strategy-making tool can be integrated into the FIVAM framework for identifying and formulating appropriate counter-measure strategies in defense planning.

References

Apostolakis, G. E., & Lemon, D. M. (2005). A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. *Risk Analysis, 25*, 361–376.

Ashford, N., Stanton, H. P. M., & Moore, C. A. (1997). *Airport operations* (2nd ed.). London: McGraw-Hill.

Axelrod, R. (1976). *Structure of decision: the cognitive maps of political elites*. Princeton University Press.

Bajpai, S., & Gupta, J. P. (2005). Site security for chemical process industries. *Journal of Loss Prevention in the Process Industries, 18*, 301–309.

Bajpai, S., & Gupta, J. P. (2007). Securing oil and gas infrastructure. *Journal of Petroleum Science and Engineering, 55*, 174–186.

Brown, T., Beyeler, W., & Barton, D. (2004). Assessing infrastructure interdependencies: The challenge of risk analysis for complex adaptive systems. *International Journal of Critical Infrastructures, 1*(1), 108–117.

Brownlow, S. A., & Watson, S. R. (1987). Structuring multiattribute value hierarchies. *Journal of Operational Research Society, 38*, 309–317.

Chen, S. J., & Hwang, C. L. (1992). *Fuzzy multiple attribute decision-making method and applications*. Berlin, Heidelberg and New York: Springer-Verlag.

Chou, S. Y., & Chang, Y. H. (2008). A decision support system for supplier selection based on a strategy-aligned fuzzy SMART approach. *Expert Systems with Applications, 34*, 2241–2253.

Dickerson, J. A., & Kosko, B. (1997). Virtual worlds as fuzzy cognitive maps. In B. Kosko (Ed.), *Fuzzy engineering* (pp. 125–141). Upper Saddle River, NJ: Prentice Hall.

Edwards, W. (1971). 'Social utilities', Engineering economist, *Summer symposium series* (Vol. 6).

Edwards, W. (1977). How to use multiattribute utility measurement for social decision making. *IEEE Transactions on Systems, Man and Cybernetics, 7*, 326–340.

Edwards, W., & Barron, F. H. (1994). SMARTS and SMARTER: Improved simple methods for multi attribute utility measurement. *Organizational Behavior and Human Decision Processes, 60*, 306–325.
Ezell, B. C. (2007). Infrastructure vulnerability assessment model (I-VAM). *Risk Analysis, 27*(3), 571–583.
Garrick, B. J. et al. (2004). Confronting the risks of terrorism: Making the right decisions. *Reliability Engineering and System Safety, 86*(2), 129–176.
Kaufmann, A., & Gupta, M. M. (1991). Introduction to fuzzy arithmetic-theory and applications. New York: Van Nostrand Reinhold.
Kosko, B. (1986). Fuzzy cognitive maps. *International Journal on Man–Machine Studies, 24*(1), 65–75.
Kosko, B. (1991). *Neural networks and fuzzy systems*. Englewood Cliffs: Prentice Hall.
Lee, C. (1990). Fuzzy logic in control systems: Fuzzy logic controller, Part I and II. *IEEE Transactions on Systems, Man and Cybernetics, 20*, 404–435.
Liang, G. S. (1999). Fuzzy MCDM based on ideal and anti-ideal concepts. *European Journal of Operational Research, 112*, 682–691.
Mifflin, Houghton (2006). *The American heritage dictionary of the English language* (4th ed.). Boston: Houghton.
Min, H. J., Beyeler, W., Brown, T., Son, Y. J., & Jones, A. T. (2007). Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions, 39*, 57–71.
Murray, A. T., Matisziw, T. C., & Grubesic, T. H. (2007). Critical network infrastructure analysis: interdiction and system flow. *Journal of Geographical Systems, 9*, 103–117.
Ross, T. J. (1995). *Fuzzy logic with engineering applications*. New York: McGraw-Hill.
Salmeron, J., Wood, K., & Baldick, R. (2004). Analysis of electric grid security under terrorist threat. *IEEE Transactions on Power Systems, 19*(2), 905–912.
Sarewitz, D., Pielke, R., Jr., & Keykhah, M. (2003). Vulnerability and risk: some thoughts from a political and policy perspective. *Risk Analysis, 23*(4), 805–810.
Sharif, A. M., & Irani, Z. (2006). Exploring fuzzy cognitive mapping for IS evaluation. *European Journal of Operational Research, 173*, 1175–1187.
Stach, W., Kurgan, L., Pedrycz, W., & Reformat, P. (2005). Genetic learning of fuzzy cognitive maps. *Fuzzy Sets and Systems, 153*, 371–401.
Sugeno, M. (1985). An introductory survey of fuzzy control. *Information Sciences, 36*, 59–83.
Willis, H. H. (2007). Guiding resource allocation based on terrorism risk. *Risk Analysis, 27*(3), 597–606.
Xirogiannis, G., Stefanou, J., & Glykas, M. (2004). A fuzzy cognitive map approach to support urban design. *Expert Systems with Applications, 26*, 257–268.
Yetton, P., & Botter, P. (1983). The relationships among group size, member ability, social decision schemes, and performance. *Organizational Behavior and Human Performance*(October), 145–159.
Yoon, K. P., & Hwang, C. L. (1995). *Multiple attribute decision making: An introduction*. Thousand Oaks, CA: Sage Publications.
Zadeh, L. A. (1975). The concept of a linguistic variable and its application to approximate reasoning. *Information Sciences*, Part 1: 8, 199–249; Part 2: 8, 301–357; Part 3: 9, 43–80.