# A Fuzzy Cyber-Risk Analysis Model for Assessing Attacks on the Availability and Integrity of the Military Command and Control Systems

*Madjid Tavana, La Salle University, Philadelphia, PA, USA & University of Paderborn, Paderborn, Germany*

*Dawn A. Trevisani, Air Force Research Laboratory, Rome, NY, USA*

*Dennis T. Kennedy, La Salle University, Philadelphia, PA, USA*

## ABSTRACT

*The increasing complexity in Military Command and Control (C2) systems has led to greater vulnerability due to system availability and integrity caused by internal vulnerabilities and external threats. Several studies have proposed measures of availability and integrity for the assets in the C2 systems using precise and certain measures (i.e., the exact number of attacks on the availability and the integrity, the number of countermeasures for the availability and integrity attacks, the effectiveness of the availability and integrity countermeasure in eliminating the threats, and the financial impact of each attack on the availability and integrity of the assets). However, these measures are often uncertain in real-world problems. The source of uncertainty can be vagueness or ambiguity. Fuzzy logic and fuzzy sets can represent vagueness and ambiguity by formalizing inaccuracies inherent in human decision-making. In this paper, the authors extend the risk assessment literature by including fuzzy measures for the number of attacks on the availability and the integrity, the number of countermeasures for the availability and integrity attacks, and the effectiveness of the availability and integrity countermeasure in eliminating these threats. They analyze the financial impact of each attack on the availability and integrity of the assets and propose a comprehensive cyber-risk assessment system for the Military C2 in the fuzzy environment.*

*Keywords:* *Availability, Command and Control System, Fuzzy Logic, Fuzzy Sets, Integrity, Risk Assessment*

DOI: 10.4018/ijban.2014070102

## INTRODUCTION

The military Command and Control (C2) systems are generally subject to high failure rates because the complex interactions among their components cannot be thoroughly planned, understood, anticipated and guarded against. Availability in military C2 systems is defined as "assured access by authorized users" and integrity is defined as "protection from unauthorized change" (Armistead, 2004, p. 71). Cyber-attacks have a direct impact on the C2 systems in terms of availability and integrity and several approaches have been suggested to eliminate or minimize them. Most system availability and integrity studies in the literature use *precise and certain* measures (i.e., the exact number of attacks on the availability and the integrity, the number of countermeasures for the availability and integrity attacks, the effectiveness of the availability and integrity countermeasure in eliminating the threats, and the financial impact of each attack on the availability and integrity of the assets). However, these measures are often uncertain in real-world problems. The source of uncertainty can be vagueness or ambiguity. Fuzzy logic and fuzzy sets can be used to represent vague and ambiguous information and formalize inaccuracy and uncertainty in human decision-making.

We develop a risk analysis model for assessing cyber-attacks on the availability and integrity of the military C2 systems. We measure availability and integrity and use an interactive model to plot the fuzzy availability and fuzzy integrity measures in a Cartesian coordinate system for various time periods. We identify whether the C2 system is in the possession, preservation, restoration, or devastation state. The remainder of this paper is organized as follows. We first provide a high-level overview of the existing approaches to operational risk quantification. The mathematical details of the cyber-risk analysis model proposed in this study is presented next. We then demonstrate a case study to exhibit the efficacy of the procedures and algorithms and show the applicability of the proposed method. We conclude with our conclusions.

## LITERATURE REVIEW

Several methods have been proposed in the literature to deal with imperfect data. Imperfect data can be characterized as being imprecise or uncertain. Other types of imperfect data such as vague or ambiguous data can be considered a special form of imprecision or uncertainty (Smets, 1997). Bayesian theory is often used to deal with both imprecision and uncertainty (Fienberg, 2006; Howson & Urbach, 1993; Jaynes, 2003). The theory of evidence is also used to deal with data that contains both imprecision and uncertainty at the same time (Shafer, 1976; Dempster, 1967). However, rough sets theory is used to handle imprecision when uncertainty is involved but cannot be quantified (Pawlak, 1991). The theory of possibility is used to handle incomplete data, which is a combination of imprecise and uncertain data (Zadeh, 1978). In contrast with these theories that can only handle one type of imperfection, random sets and the conditional event algebra can handle all types of imperfect data (Goodman et al., 1997). We use fuzzy values in our model to represent vagueness and ambiguity. Fuzzy logic enables computation in the face of vagueness and ambiguity, generating approximate results (Nedjah & Mourelle, 2005). While uncertainty represents the state of knowledge about a piece of data, imprecision is the characteristic of the data that cannot be expressed with a single value. The theory of fuzzy sets has been proposed by Zadeh (1965) to deal with vague data which is a particular form of both imprecise and uncertain data. Fuzzy sets have been used to account for the vague data in various work flow management systems (Lin et al., 2007; Tsai & Wang, 2008). The membership function of a fuzzy set defines the mapping of inputs to the degree or strength of membership, ranging from 0 to 1. The shape of this membership function can vary, as any function whose image is between 0 and 1 is a possible membership function. The most

common forms of these functions are those represented by straight lines, such as triangular and trapezoidal member functions. In the proposed method, trapezoidal fuzzy numbers are used to capture and convert the fuzzy imprecise and uncertain information. Among the various types of fuzzy numbers, trapezoidal fuzzy numbers are used most often for characterizing linguistic information in practical applications (Klir & Yuan 1995, Yeh & Deng 2004). The common use of trapezoidal fuzzy numbers is mainly attributed to their simplicity in both concept and computation.

Cyber-risk is the threat caused by a malicious electronic event that causes disruption of operations and monetary loss (Öğüt et al., 2011). Cyber-attacks have a direct impact on the availability and integrity of organizational systems. Various process approach methods including causal networks, Bayesian belief networks, and fuzzy logic have been proposed to quantify the operational risks in organizations (Smithson & Paul, 2004). The process approach focuses on identifying the risk associated with the chain of activities that comprise an operation (Salmela, 2008; Cernauskas & Tarantino, 2009; Dickstein & Flast, 2009). Other commonly used methods for risk analysis include: business process modeling (Kokolakis et al., 2000), multiple perspective enterprise modeling technique (Frank, 2002), action research and business process modeling (Salmela, 2008), design science research methodology (Strecker et al., 2011), Bayesian belief networks (Guarrao, 1987; Krieg, 2001; Baskerville, 1993; Ozeir, 1988), and fuzzy logic (Smith & Eloff, 2002; Ngai & Wat, 2005).

Most of the systems used for selecting countermeasures to block or mitigate security attacks are qualitative (Alberts & Dorofee, 2002; Egan, 2005; Bistarelli et al., 2007; Bojanc & Jerman-Blazic, 2008). Chen et al. (2011) discussed current research findings in enterprise risk and security management using mining techniques. Contrary to qualitative approaches, the literature on quantitative methods for countermeasure selection is very limited (Sawik, 2013). A few quantitative measures are proposed for quantifying risk in security vulnerabilities (Gupta et al., 2006), supply chains (Deane et al., 2009), Cyber-security (Rees et al., 2011), information technology (Rakes et al., 2012), and network security (Viduto et al., 2012).

## FUZZY CYBER-RISK ANALYSIS MODEL

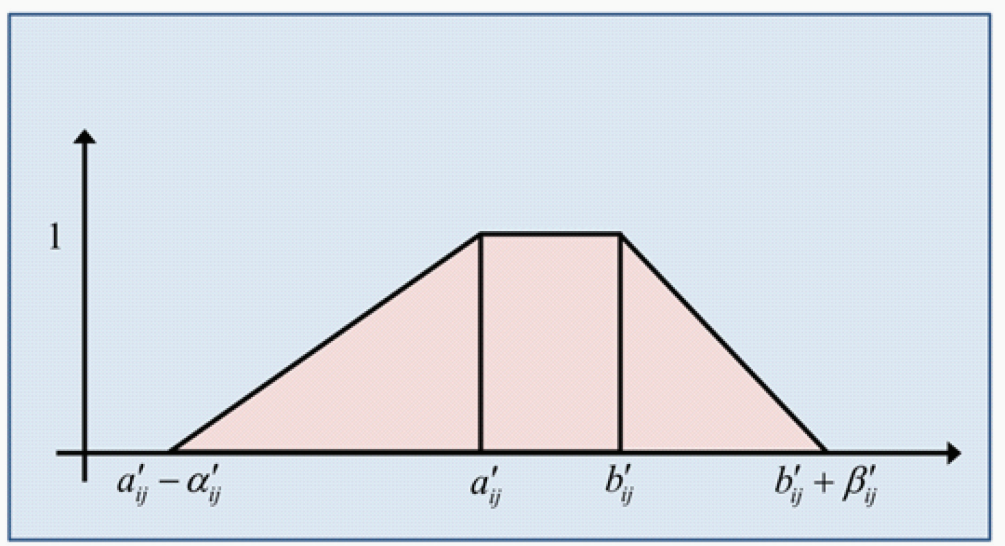
The fuzzy cyber-risk analysis model proposed in this study is an extension of the deterministic risk analysis model proposed by Tavana et al. (in press). The proposed model is composed of two components: the availability model and the integrity model. Note that the threats to the C2 systems seek to adversely affect the availability (through destruction and denial of service) and the integrity (through modification) of *n* assets $a_i (i = 1, 2, ..., n)$.

### Fuzzy Availability Model

In this section we assume that $e'_{ij}$, the effectiveness of the availability countermeasures, are trapezoidal fuzzy numbers (the case of triangular fuzzy numbers is a special case of the trapezoidal fuzzy numbers). Assume that each $e'_{ij}$ is a trapezoidal fuzzy number as follows: $e'_{ij} = (a'_{ij}, b'_{ij}, \alpha'_{ij}, \beta'_{ij})$ where $i = 1, ..., n$ and $j = 1, ..., m'_i$. $e'_{ij}$ represents the effectiveness of $c'_{ij}$ which is the countermeasure for the availability of Asset $i$ where $m'_i$ represents the number of availability measures for Asset $i$.

Each fuzzy set $e'_{ij}$ corresponds to a trapezoidal fuzzy number with tolerance interval $[a'_{ij}, b'_{ij}]$, left-width $\alpha'_{ij}$, and right-width $\beta'_{ij}$. The membership function of the trapezoidal fuzzy set $A = (a'_{ij}, b'_{ij}, \alpha'_{ij}, \beta'_{ij})$ with a continuous membership function $\mu_A(x)$, as shown in Figure 1, has the following form:

*Figure 1. Trapezoidal fuzzy numbers used in the availability model*




$$\begin{cases} 1 - \dfrac{a'_{ij} - x}{\alpha'_{ij}} & \text{if} \quad a'_{ij} - \alpha'_{ij} \le x \le a'_{ij} \\ 1 & \text{if} \quad a'_{ij} \le x \le b'_{ij} \\ 1 - \dfrac{x - b'_{ij}}{\beta'_{ij}} & \text{if} \quad b'_{ij} \le x \le b'_{ij} + \beta'_{ij} \\ 0 & \text{if} \quad \text{otherwise} \end{cases} \tag{1}$$

The financial impact of all attacks on the availability of Asset $i$, $F'_i$, is a trapezoidal fuzzy number calculated as follows:

$$F'_i = f'_i \cdot s'_i \tag{2}$$

where $i = 1,\ldots,n$ and $s'_i = t'_i\left(1 - \prod_{j=1}^{m_i} e'_{ij}\right)$.

$s'_i$ is a trapezoidal fuzzy number which represents the number of successful attacks on the availability of Asset $i$ per year, $t'_i$ is a crisp number representing the number of attacks per year on the availability of Asset $i$, and $f'_i$ is a crisp number representing the cost of each successful attack on the availability of asset *i*. We can use the fuzzy arithmetic proposed by Dubois and Prade (1980) to calculate:

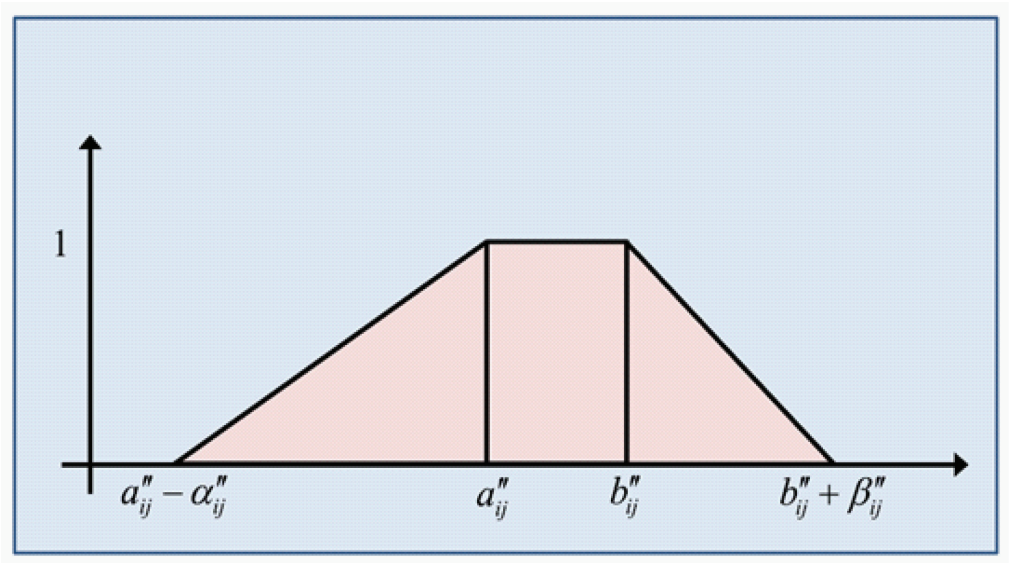
$$F'_i = f'_i \cdot s'_i = f'_i \cdot t'_i\left(1 - \prod_{j=1}^{m'_i} e'_{ij}\right) \tag{3}$$

According to the fuzzy arithmetic of Dubois and Prade (1980) we can multiply two trapezoidal fuzzy numbers as follows:

$$A_1 \otimes A_2 = (a_1, b_1, \alpha_1, \beta_1) \otimes (a_2, b_2, \alpha_2, \beta_2) = (a_1 a_2, b_1 b_2, a_1\alpha_2 + a_2\alpha_1 - \alpha_1\alpha_2, b_1\beta_2 + b_2\beta_1 + \beta_1\beta_2) \tag{4}$$

We use this arithmetic to calculate $\prod_{j=1}^{m'_i} e'_{ij}$ where $e'_{ij}$ is the trapezoidal fuzzy number $(a'_{ij}, b'_{ij}, \alpha'_{ij}, \beta'_{ij})$. Let $p'_{il} = \prod_{j=1}^{l'} e'_{ij}$ where $l = 1,\ldots,m'_i$.

*Figure 2. Trapezoidal fuzzy numbers used in the integrity model*




Note that $p'_{i1} = e'_{i1}$, $p'_{il} = e'_{il} \otimes (p_{i,l-1})$, and $p'_{i,m_i} = \prod_{j=1}^{m'_i} e'_{ij}$.

We can calculate $p'_{il}$ $(l = 1,...,m'_i)$ recursively using the fuzzy arithmetic of Dubois and Prade (1980). Let $p'_{il} = (a'_{p'_{il}}, b'_{p'_{il}}, \alpha'_{p'_{il}}, \beta'_{p'_{il}})$,

$$\begin{aligned} p'_{il'} &= e'_{il} \otimes (p'_{i,l-1}) \\ &= (a'_{il}, b'_{il}, \alpha'_{il}, \beta'_{il}) \otimes (a'_{p'_{i,l-1}}, b'_{p'_{i,l-1}}, \alpha'_{p'_{i,l-1}}, \beta'_{p'_{i,l-1}}) \\ &= (a'_{il}a'_{p'_{i,l-1}}, b'_{il}b'_{p'_{i,l-1}}, a'_{il}\alpha'_{p'_{i,l-1}} + a'_{p'_{i,l-1}}\alpha'_{il} \\ &\quad -\alpha'_{il}\alpha'_{p'_{i,l-1}}, b'_{il}\beta'_{p'_{i,l-1}} + b'_{p'_{i,l-1}}\beta'_{il} + \beta'_{il}\beta'_{p'_{i,l-1}}) \end{aligned} \quad (5)$$

where $l = 2,...,m'_i$. $p'_{il}$ is calculated recursively for $l = 2,...,m'_i$. Note that $p'_{i,m'_i} = \prod_{j=1}^{m'_i} e'_{ij}$. Let $p'_{i,m'_i} = (a'_{p'_{i,m'_i}}, b'_{p'_{i,m'_i}}, \alpha'_{p'_{i,m'_i}}, \beta'_{p'_{i,m'_i}})$. According to the fuzzy arithmetic of Dubois and Prade (1980):

$$1 - p'_{i,m'_i} = (1 - b'_{p'_{i,m'_i}}, 1 - a'_{p'_{i,m'_i}}, \beta'_{p'_{i,m'_i}}, \alpha'_{p'_{i,m'_i}}) \quad (6)$$

$$F'_i = f'_i t'_i (1 - \prod_{j=1}^{m'_i} e'_{ij}) = f'_i t'_i (1 - p'_{i,m'_i}) \quad (7)$$

Therefore $F'_i$ is a trapezoidal fuzzy number that can be represented as follows:

$$\begin{aligned} F'_i = \\ (f'_i t'_i (1 - b'_{p'_{i,m'_i}}), f'_i t'_i (1 - a'_{p'_{i,m'_i}}), f'_i t'_i \beta'_{p'_{i,m'_i}}, f'_i t'_i \alpha'_{p'_{i,m'_i}}) \end{aligned} \quad (8)$$

We can then transform $F'_i$ into a crisp number using the center of gravity method. The center of gravity for the trapezoidal fuzzy set $A = (a'_{ij}, b'_{ij}, \alpha'_{ij}, \beta'_{ij})$ can be calculated as follows (see the derivation in the Appendix):

$$cg(A) = \frac{a'_{ij}(3a'_{ij} - a'_{ij}) + \beta'_{ij}(\beta'_{ij} + 3b'_{ij}) + 3(b'^2_{ij} - a'^2_{ij})}{3\left[\alpha'_{ij} + \beta'_{ij} + 2(b'_{ij} - a'_{ij})\right]} \quad (9)$$

Accordingly, the center of gravity of $F'_i$ can be defined as follows:

$$cg(F'_i) = \frac{\begin{array}{l} f'_i t'_i b'_{p'_{i,m'_i}}[3(1 - b'_{p'_{i,m'_i}}) - \beta'_{p'_{i,m'_i}}] \\ + f'_i t'_i \alpha'_{p'_{i,m'_i}}[\alpha'_{p'_{i,m'_i}} + 3(1 - a'_{p'_{i,m'_i}})] \\ + 3f'_i t'_i[(1 - \alpha'_{p'_{i,m'_i}})^2 - (1 - b'_{p'_{i,m'_i}})^2] \end{array}}{3[\beta'_{p'_{i,m'_i}} + \alpha'_{p'_{i,m'_i}} + 2(b'_{p'_{i,m'_i}} - a'_{p'_{i,m'_i}})]} \quad (10)$$

Note that $cg(F'_i) = f'_i t'_i cg(1 - p'_{i,m'_i})$.

## Fuzzy Integrity Model

In the integrity model, $e''_{ij}$, the effectiveness of the integrity countermeasures, are trapezoidal fuzzy numbers. Assume that each $e''_{ij}$ is a trapezoidal fuzzy number as follows:

$$e''_{ij} = (a''_{ij}, b''_{ij}, \alpha''_{ij}, \beta''_{ij})$$

where $i = 1,...,n$ and $j = 1,...,m''_i$. $e''_{ij}$ represents the effectiveness of $c''_{ij}$ which is the countermeasure for the integrity of Asset $i$ where $m''_i$ represents the number of integrity measures for Asset $i$. Each fuzzy set $e''_{ij}$ corresponds to a trapezoidal fuzzy number with tolerance interval $[a''_{ij}, b''_{ij}]$, left-width $\alpha''_{ij}$, and right-width $\beta''_{ij}$. The membership function of the trapezoidal fuzzy set $A = (a''_{ij}, b''_{ij}, \alpha''_{ij}, \beta''_{ij})$ with a continuous membership function $\mu_A(x)$, as shown in Figure 1, has the following form:

$$\begin{cases} 1 - \dfrac{a''_{ij} - x}{\alpha''_{ij}} & \text{if} \quad a''_{ij} - \alpha''_{ij} \le x \le a''_{ij} \\ 1 & \text{if} \quad a''_{ij} \le x \le b''_{ij} \\ 1 - \dfrac{x - b''_{ij}}{\beta''_{ij}} & \text{if} \quad b''_{ij} \le x \le b''_{ij} + \beta''_{ij} \\ 0 & \text{if} \quad \text{otherwise} \end{cases} \quad (11)$$

The financial impact of all attacks on the integrity of Asset $i$, $F''_i$, is a trapezoidal fuzzy number calculated as follows:

$$F''_i = f''_i \cdot s''_i \quad (12)$$

where $i = 1,...,n$ and $s''_i = t''_i\left(1 - \prod_{j=1}^{m''_i} e''_{ij}\right)$.

$s''_i$ is a trapezoidal fuzzy number which represents the number of successful attacks on the integrity of Asset $i$ per year, $t''_i$ is a crisp number representing the number of attacks per year on the integrity of Asset $i$, and $f''_i$ is a crisp number representing the cost of each successful attack on the integrity of asset $i$. We can use the fuzzy arithmetic proposed by Dubois and Prade (1980) to calculate:

$$F''_i = f''_i \cdot s''_i = f''_i \cdot t''_i\left(1 - \prod_{j=1}^{m''_i} e''_{ij}\right) \quad (13)$$

We use the fuzzy arithmetic of Dubois and Prade(1980)tocalculate $\prod_{j=1}^{m''_i} e''_{ij}$ .Let $p''_{il} = \prod_{j=1}^{l''} e''_{ij}$ where $l = 1,...,m''_i$. Note that $p''_{i1} = e''_{i1}$, $p''_{il} = e''_{il} \otimes (p_{i,l-1})$, and $p''_{i,m''_i} = \prod_{j=1}^{m''_i} e''_{ij}$. We calculate $p''_{il}$ $(l = 1,...,m''_i)$ recursively. Let $p''_{il} = (a''_{p''_{il}}, b''_{p''_{il}}, \alpha''_{p''_{il}}, \beta''_{p''_{il}})$,

$$p''_{il} = e''_{il} \otimes (p''_{i,l-1})$$
$$= (a''_{il}, b''_{il}, \alpha''_{il}, \beta''_{il}) \otimes (a''_{p'_{i,l-1}}, b''_{p'_{i,l-1}}, \alpha''_{p'_{i,l-1}}, \beta''_{p'_{i,l-1}})$$

$$= (a'_{il} a'_{p''_{i,l-1}}, b'_{il} b'_{p''_{i,l-1}}, a'_{il} \alpha'_{p''_{i,l-1}} + a''_{p''_{i,l-1}} \alpha''_{il}$$
$$-\alpha''_{il} \alpha''_{p''_{i,l-1}}, b''_{il} \beta''_{p''_{i,l-1}} + b''_{p''_{i,l-1}} \beta''_{il} + \beta''_{il} \beta''_{p''_{i,l-1}}) \quad (14)$$

where $l = 2,...,m''_i$.

$p''_{il}$ is calculated recursively for $l = 2,...,m''_i$. Note that $p''_{i,m''_i} = \prod_{j=1}^{m''_i} e''_{ij}$. Let $p''_{i,m''_i} = (a''_{p''_{i,m''_i}}, b''_{p''_{i,m''_i}}, \alpha''_{p''_{i,m''_i}}, \beta''_{p''_{i,m''_i}})$. According to the fuzzy arithmetic of Dubois and Prade (1980):

$$1 - p''_{i,m''_i} = (1 - b''_{p''_{i,m''_i}}, 1 - a''_{p''_{i,m''_i}}, \beta''_{p''_{i,m''_i}}, \alpha''_{p''_{i,m''_i}}) \quad (15)$$

$$F''_i = f''_i t''_i (1 - \prod_{j=1}^{m''_i} e''_{ij}) = f''_i t'' (1 - p''_{i,m''_i}) \quad (16)$$

Therefore $F''_i$ is a trapezoidal fuzzy number that can be represented as follows:

$$F''_i = (f''_i t''_i (1 - b''_{p''_{i,m''_i}}), f''_i t''$$
$$(1 - a''_{p''_{i,m''_i}}), f''_i t'' \beta''_{p''_{i,m''_i}}, f''_i t'' \alpha''_{p''_{i,m''_i}}) \quad (17)$$

We can then transform $F''_i$ into a crisp number using the center of gravity method as follows:

$$cg(A) = \frac{a''_{ij}(3a''_{ij} - a''_{ij}) + \beta''_{ij}(\beta''_{ij} + 3b''_{ij}) + 3(b''^2_{ij} - a''^2_{ij})}{3\left[\alpha''_{ij} + \beta''_{ij} + 2(b''_{ij} - a''_{ij})\right]} \quad (18)$$

Accordingly, the center of gravity of $F''_i$ can be defined as follows:

$$cg(F''_i) = \frac{\begin{array}{l} f''_i t''_i b''_{p''_{i,m''_i}} [3(1 - b''_{p''_{i,m''_i}}) - \beta''_{p''_{i,m''_i}}] \\ + f''_i t''_i \alpha''_{p''_{i,m''_i}} [\alpha''_{p''_{i,m''_i}} + 3(1 - \alpha''_{p''_{i,m''_i}})] \\ + 3 f''_i t''_i [(1 - \alpha''_{p''_{i,m''_i}})^2 - (1 - b''_{p''_{i,m''_i}})^2] \end{array}}{3[b''_{p''_{i,m''_i}} + \alpha''_{p''_{i,m''_i}} + 2(b''_{p''_{i,m''_i}} - \alpha''_{p''_{i,m''_i}})]} \quad (19)$$

Note that $cg(F''_i) = f''_i t''_i cg(1 - p''_{i,m''_i})$.

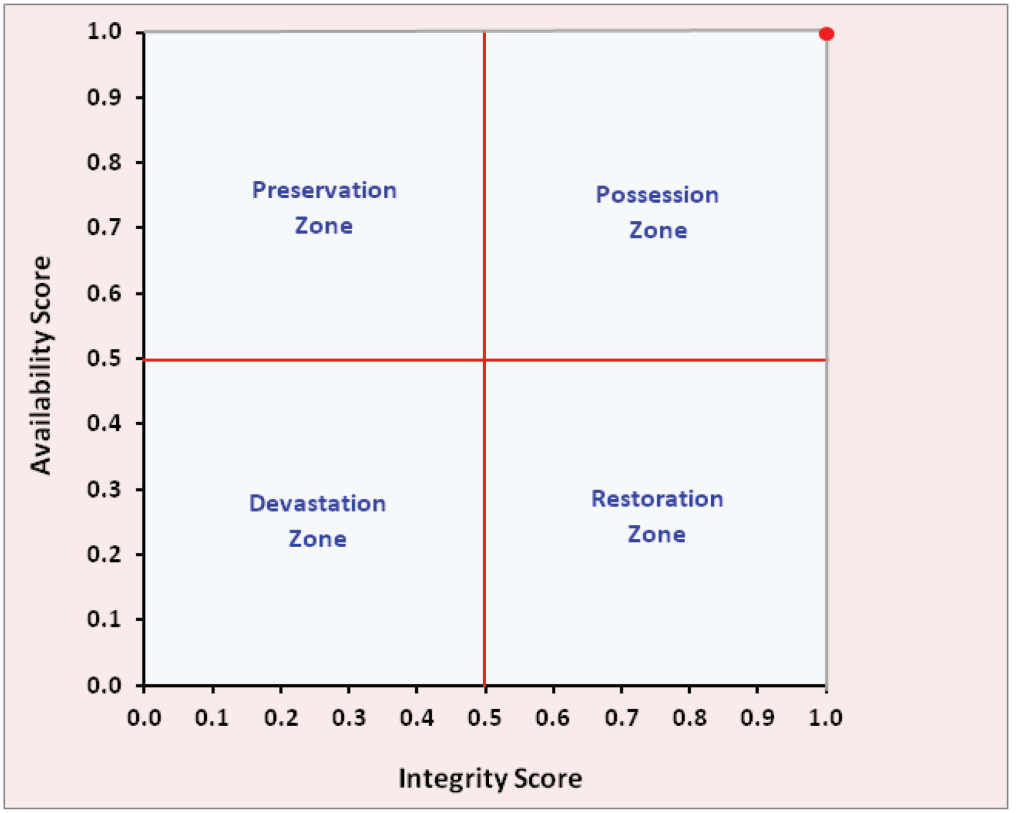
We can then find the availability and integrity indices of the C2 system for different time periods by standardizing the expected financial impacts of the availability $\left(F'_{i_k}\right)$ and the integrity $\left(F''_{i_k}\right)$ cases for a comparative analysis for different assets over $k$ periods $(k = 1,...,K)$. There are several methods for standardizing these expected financial impact figures. We adopt the most frequently used procedure that uses the minimum and maximum scores as scaling points (e.g., Carver, 1991; Malczewski, 1996). Eq. (20) is used to calculate the availability score for Asset $i$ at time period $k$ and Eq. (21) is used to calculate the integrity score of Asset $i$ at time period $k$ as follows:

$$F'_{i_k} = \frac{F'_{i_k} - F'^{\min}_{i_k}}{F'^{\max}_{i_k} - F'^{\min}_{i_k}} \quad (20)$$

$$F''_{i_k} = \frac{F''_{i_k} - F''^{\min}_{i_k}}{F''^{\max}_{i_k} - F''^{\min}_{i_k}} \quad (21)$$

We then plot the $F'_{i_k}$ and $F''_{i_k}$ indices on a Cartesian coordinate system for different time periods. The availability indices are plotted on the $x$-axis and the integrity indices are plotted on the $y$-axis. The average availability and integrity indices divide this plane into four quadrants, identified as the Possession, Preservation, Restoration and Devastation Quadrants. The best point (ideal point) on this grid is the point (1,1) where both the availability

*Figure 3. A graphical representation of the C2 system states in the proposed model*




and integrity indices are at their maximum value (see Figure 3).

- **Possession Quadrant:** the C2 system in this quadrant has above average availability and integrity.
- **Preservation Quadrant:** the C2 system in this quadrant has above average availability and below average integrity.
- **Restoration Quadrant:** the C2 system in this quadrant has below average availability and above average integrity.
- **Devastation Quadrant:** the C2 system in this quadrant has below average availability and integrity.

## CASE STUDY

Let us consider a hypothetical C2 system with two assets $(a_1, a_2)$. The average threat against the availability of $a_1$ (Asset 1) occurs at the rate of 100 attacks per year $(t_1' = 100)$. The expected financial impact of each successful attack on the availability Asset 1 is \$5000 $(f_1' = 5000)$. We have two availability countermeasures of $c_{11}'$ and $c_{12}'$ for Asset 1 with the following fuzzy effectiveness scores:

$$e_{11}' = (.7,.9,.1,.1)$$

$$e_{12}' = (.5,.7,.1,.2)$$

*Table 1. The expected financial impact of the attacks on the availability and integrity*

| Week | Expected financial loss | | Availability Score | Integrity Score |
|---|---|---|---|---|
| | Availability | Integrity | | |
| 1 | 206,640 | 0 | 0.813 | 0.000 |
| 2 | 206,640 | 285,374 | 0.813 | 0.956 |
| 3 | 240,274 | 291,474 | 0.946 | 0.977 |
| 4 | 254,016 | 286,897 | 1.000 | 0.962 |
| 5 | 250,182 | 225,543 | 0.985 | 0.756 |
| 6 | 53,897 | 213,626 | 0.212 | 0.716 |
| 7 | 250,182 | 184,347 | 0.985 | 0.618 |
| 8 | 82,389 | 272,129 | 0.324 | 0.912 |
| 9 | 222,208 | 274,391 | 0.875 | 0.920 |
| 10 | 53,897 | 274,391 | 0.212 | 0.920 |
| 11 | 222,208 | 207,890 | 0.875 | 0.697 |
| 12 | 250,182 | 264,246 | 0.985 | 0.886 |
| 13 | 198,088 | 158,883 | 0.780 | 0.533 |
| 14 | 238,758 | 213,626 | 0.940 | 0.716 |
| 15 | 0 | 0 | 0.000 | 0.000 |
| 16 | 254,016 | 298,368 | 1.000 | 1.000 |
| 17 | 238,758 | 285,374 | 0.940 | 0.956 |
| 18 | 206,640 | 184,347 | 0.813 | 0.618 |
| 19 | 248,270 | 225,543 | 0.977 | 0.756 |
| 20 | 198,088 | 274,391 | 0.780 | 0.920 |
| 21 | 248,270 | 291,474 | 0.977 | 0.977 |
| 22 | 232,711 | 264,246 | 0.916 | 0.886 |
| 23 | 222,208 | 225,543 | 0.875 | 0.756 |
| 24 | 232,711 | 298,368 | 0.916 | 1.000 |
| 25 | 0 | 291,474 | 0.000 | 0.977 |
| 26 | 248,270 | 274,391 | 0.977 | 0.920 |
| 27 | 238,758 | 158,883 | 0.940 | 0.533 |
| 28 | 254,016 | 0 | 1.000 | 0.000 |
| 29 | 217,737 | 207,890 | 0.857 | 0.697 |
| 30 | 206,640 | 285,374 | 0.813 | 0.956 |
| 31 | 233,465 | 0 | 0.919 | 0.000 |
| 32 | 238,758 | 285,374 | 0.940 | 0.956 |
| 33 | 222,208 | 272,129 | 0.875 | 0.912 |
| 34 | 233,465 | 213,626 | 0.919 | 0.716 |
| 35 | 217,737 | 274,391 | 0.857 | 0.920 |
| 36 | 240,274 | 225,543 | 0.946 | 0.756 |

*continued on following page*

*Table 1. Continued*

| Week | Expected financial loss | | Availability Score | Integrity Score |
|---|---|---|---|---|
| | Availability | Integrity | | |
| 37 | 248,270 | 272,129 | 0.977 | 0.912 |
| 38 | 250,182 | 213,626 | 0.985 | 0.716 |
| 39 | 136,265 | 272,129 | 0.536 | 0.912 |
| 40 | 0 | 225,543 | 0.000 | 0.756 |
| 41 | 222,208 | 184,347 | 0.875 | 0.618 |
| 42 | 206,640 | 225,543 | 0.813 | 0.756 |
| 43 | 248,270 | 207,890 | 0.977 | 0.697 |
| 44 | 217,737 | 264,246 | 0.857 | 0.886 |
| 45 | 174,034 | 207,890 | 0.685 | 0.697 |
| 46 | 233,465 | 272,129 | 0.919 | 0.912 |
| 47 | 53,897 | 264,246 | 0.212 | 0.886 |
| 48 | 198,088 | 158,883 | 0.780 | 0.533 |
| 49 | 217,737 | 207,890 | 0.857 | 0.697 |
| 50 | 0 | 207,890 | 0.000 | 0.697 |
| 51 | 136,265 | 274,391 | 0.536 | 0.920 |
| 52 | 82,389 | 291,474 | 0.324 | 0.977 |
| **Average** | **192,077** | **225,765** | **0.756** | **0.757** |

The average threats against the availability of $a_2$ (Asset 2) occurs at the rate of 50 attacks per year $(t_2' = 50)$. The expected financial impact of each successful attack on the availability of Asset 2 is \$6000 $(f_2' = 6000)$. We have three availability countermeasures of $(c_{21}', c_{22}'$ and $c_{23}')$ for Asset 2 with the following fuzzy effectiveness scores:

$$e_{21}' = (.05,.15,.05,.1)$$
$$e_{22}' = (.25,.35,.1,.1)$$
$$e_{23}' = (.3,.5,.3,.4)$$

To calculate $cg(F_1')$ we find:

$$p_{11}' = e_{11}' = (.7,.9,.1,.1)$$
$$p_{12}' = e_{12}' \otimes e_{11}' = (.5,.7,.1,.2) \otimes (.7,.9,.1,.1)$$
$$= ((.5)(.7),(.7)(.9),(.5)(.1) + (.7)(.1)$$
$$-(.1)(.1),(.7)(.1) + (.9)(.2) + (.1)(.2))$$
$$= (.36,.63,.1,.27)$$

Next we use

$$F_i' = (f_i t_i'(1 - b_{p_{i,m_i}'}'), f_i t_i'(1 - a_{p_{i,m_i}'}'), f_i t_i' \beta_{p_{i,m_i}'}', f_i t_i' \alpha_{p_{i,m_i}'}')$$

and find $F_i'$ as follows:

$$F_1' = (f_1 t_1'(1 - \prod_{j=1}^{2} e_{ij}') = f_1 t_1'(1 - p_{12}')$$
$$= (f_1 t_1'[1 - (.35,.63,.1,.2)] = f_1 t_1'(.37,.67,.27,.1)$$

$$cg[(.37,.65,.27,.1)] = \frac{\begin{array}{l}.27(3(.37)-.27)\\ +.1(.1+3(.65))\\ +3((.65)^2-(.37)^2)\end{array}}{3[.27+.1+2(.65-.37)]}$$

$$= .4619$$

$$cg(F_1') = f_1't_1'(.4619) = (5000)(100) = \$230,950$$

To calculate $cg(F_1')$ we similarly find:

$$p_{21}' = e_{21}' = (.05,.15,.05,.1)$$

$$p_{22}' = e_{22}' \otimes e_{21}'$$
$$= (.25,.35,.1,.1) \otimes (.05,.15,.05,.1)$$
$$= ((.25)(.05),(.35)(.15),(.25)(.05)+(.05)(.1)$$
$$-(.1)(.05),(.35)(.1)+(.15)(.1)+(.1)(.1))$$

$$= (.0125,.0525,.0125,.06)$$

$$p_{23}' = e_{23}' \otimes p_{22}'$$
$$= (.3,.5,.3,.4) \otimes (.0125,.0525,.125,.06)$$
$$= ((.3)(.0125),(.5)(.0525),(.3)(.0125)+(.0125)(.3)$$
$$-(.3)(.0125),(.5)(.06)+(.0125)(.4)+(.4)(.06))$$

$$= (.00375,.02625,.0375,.075)$$

$$F_2' = (f_2't_2'(1-\prod_{j=1}^{3} e_{ij}') = f_2't_2'(1-p_{23}')$$
$$= (f_2't_2'[1-(.00375,.02625,.0375,.075)]$$
$$= f_2't_2'(.97375,.99625,.075,.0375)$$

$$cg[(.97375,.99625,.075,.0375)] = \frac{\begin{array}{l}.057(3(.9737)-.075)\\ +.0375(.0375+3(.99625))\\ +3((.99625)^2-(.97375)^2)\end{array}}{3[.075+.0375+2(.99625-.97375)]}$$

$$= .8649$$

$$cg(F_2') = f_2't_2'(.86493)$$
$$= (6000)(50)(.86493) = \$259,479$$

The expected financial loss caused by the attack on the availability of Assets 1 and 2 are \$260,000 and \$296,400, respectively for the crisp case:

$$F_1' = f_1't_1'[(1-(.8)(.6)] = (5000)(100)(.52)$$
$$= \$260,000$$

$$F_2' = f_2't_2'[(1-(.1)(.3)(.4)] = (6000)(50)(.988)$$
$$= \$296,400$$

The expected financial loss caused by the attack on the availability of Assets 1 and 2 are $cg(F_1') = \$230,950$ and $cg(F_2') = \$259,479$, respectively for the fuzzy case.

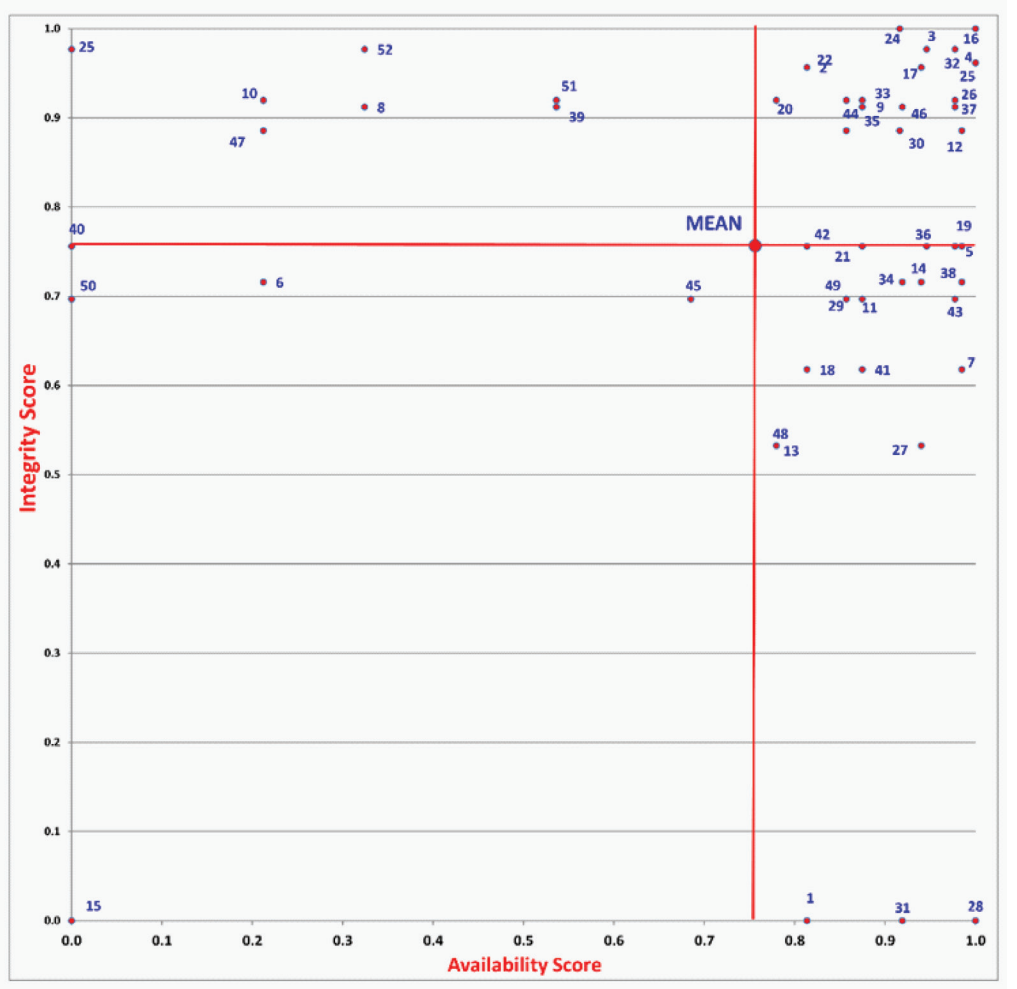
Next, we ran a simulation study for one year (52 weeks) and standardized the expected financial impacts of the availability and integrity scenarios presented in Table 1.

We then plotted the results of the simulation study for 52 weeks in Figure 2. Figure 4 presents a snapshot of the C2 system over a 52 week assessment period. As shown in Figure 4, the C2 system simulated in this study was in the possession state for 22 weeks (42%), the devastation state for 4 weeks (7.5%), the preservation state for 8 weeks (15.5%), and the restoration state for 18 weeks (35%).

## CONCLUSION

The necessity for readiness and the ability to cope with the possibility of cyber-attack in military C2 systems are important areas for future system availability and integrity studies. The literature describes two main reasons why adequate progress has not been made on developing risk analysis methods for information systems. First, most managers have no proven and reliable method for measuring the effectiveness of their countermeasures (Baker et al., 2007). Second, most managers are uncomfortable with supplying precise values related to future events which they know to be imprecise or uncertain (Baker et al., 2007). We proposed a risk assessment model for considering the

*Figure 4. A snapshot of the C2 system over a 52 week assessment period*




number of attacks on the availability and the integrity, the number of countermeasures for the availability and integrity attacks, and the effectiveness of the availability and integrity countermeasure in eliminating these threats. We used fuzzy logic and fuzzy sets to represent vagueness and ambiguity by formalizing inaccuracies inherent in human decision-making. We analyzed the financial impact of each attack on the availability and integrity of the assets. We used a case study to exhibit the efficacy of the procedures and demonstrate the applicability of the proposed method.

## ACKNOWLEDGMENT

This research was supported by the U.S. Air Force Research Laboratory grant number FA8750-13-2-0115. The authors would like to thank the anonymous reviewers and the editor for their insightful comments and suggestions.

## REFERENCES


Alberts, C. J., & Dorofee, A. J. (2002). *Managing Information Security Risks: The OCTAVE Approach*. Upper Saddle River, New Jersey: Pearson Education, Inc.

Baker, W. H., Rees, L. P., & Tippett, P. S. (2007). Necessary measures: Metric-driven information security risk assessment and decision making. *Communications of the ACM*, *50*(10), 101–106. doi:10.1145/1290958.1290969

Baskerville, R. L. (1993). Information systems security design methods: Implication for information systems development. *ACM Computing Surveys*, *25*(4), 375–414. doi:10.1145/162124.162127

Bistarelli, S., Fioravanti, F., & Peretti, P. (2007). Using cp-nets as a guide for countermeasure selection. *Proceedings of the 2007 ACM Symposium on Applied Computing*, Seoul, Korea, 300–304. doi:10.1145/1244002.1244073

Bojanc, R., & Jerman-Blazic, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, *28*(5), 413–422. doi:10.1016/j.ijinfomgt.2008.02.002

Carver, S. J. (1991). Integrating multi-criteria evaluation with geographical Information Systems. *International Journal of Geographical Information Systems*, *5*(3), 321–339. doi:10.1080/02693799108927858

Cernauskas, D., & Tarantino, A. (2009). Operational risk management with process control and business process modeling. *The Journal of Operational Risk*, *4*(2), 1–22.

Chen, H., Chau, M., & Li, S. (2011). Enterprise risk and security management: Data, text and web mining. *Decision Support Systems*, *50*(4), 649–650. doi:10.1016/j.dss.2010.08.026

Deane, J. K., Ragsdale, C. T., Rakes, T. R., & Rees, L. P. (2009). Managing supply chain risk and disruption from IT security incidents. *Operations Management Research*, *2*(1), 4–12. doi:10.1007/s12063-009-0018-2

Dempster, A. (1967). Upper and lower probabilities induced by multivalued mapping. *Annals of Mathematical Statistics*, *38*(2), 325–339. doi:10.1214/aoms/1177698950

Dickstein, D. I., & Flast, R. H. (2009). *No Excuses: A Business Process Approach to Managing Operational Risk*. Hoboken, New Jersey: John Willey and Sons Inc.

Dubois, D., & Prade, H. (1980). *Operations on fuzzy numbers. Fuzzy Sets and System: Theory and Applications*. New York: Academic Press.

Egan, M. (2005). *The Executive Guide to Information Security*. Indianapolis, IN: Symantec Press.

Fienberg, S. E. (2006). When Did Bayesian Inference Become "Bayesian"? *Bayesian Analysis*, *1*(1), 1–40. doi:10.1214/06-BA101

Frank, U. (2002). Multi-perspective enterprise modeling (MEMO): conceptual framework and modeling languages, Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS), IEEE Computer Society Washington, DC, USA, Honolulu, HI, 72–82.

Goodman, I., Mahler, R. P. S., & Nguyen, H. (1997). *Mathematics of data fusion*. Dordrecht: Kluwer Academic Publishers. doi:10.1007/978-94-015-8929-1

Guarrao, S. (1987). Principles and procedures of the LRAM approach to information systems risk analysis and management. *Computers & Security*, *6*(6), 493–504. doi:10.1016/0167-4048(87)90030-7

Gupta, M., Rees, J., Chaturvedi, A., & Chi, J. (2006). Matching information security vulnerabilities to organizational security profiles: A genetic algorithm approach. *Decision Support Systems*, *41*(3), 592–603. doi:10.1016/j.dss.2004.06.004

Howson, C., & Urbach, P. (1993). *Scientific reasoning: The Bayesian approach*. Chicago: Open Court.

Jaynes, E. T. (2003). Probability theory: The logic of science, In the art of scientific computing, G.L. Bretthorst (Ed.), Cambridge University Press, New York.

Klir, G. J., & Yuan, B. (1995). *Fuzzy sets and fuzzy logic: Theory and applications*. New York: Prentice-Hall.

Kokolakis, S. A., Demopoulos, A. J., & Kiountouzis, E. A. (2000). The use of business process modelling in information systems security analysis and design. *Information Management & Computer Security*, *8*(3), 107–116. doi:10.1108/09685220010339192

Krieg, M. L. (2001). *A Tutorial on Bayesian Belief Networks. Technical Note DSTO-TN-0403*. Edinburgh, South Australia: DSTO Electronics and Surveillance Laboratory.

Lin, H.-Y., Hsu, P.-Y., & Sheen, G.-J. (2007). A fuzzy-based decision-making procedure for data warehouse system selection. *Expert Systems with Applications*, *32*(3), 939–953. doi:10.1016/j.eswa.2006.01.031

Malczewski, J. (1996). A GIS-based approach to multiple criteria group decision making. *International Journal of Geographical Information Systems*, *10*(8), 955–971. doi:10.1080/02693799608902119

Nedjah, N., Mourelle, L., & de, .M. (2005). Introducing you to fuzziness. *Studies in Fuzziness and Soft Computing*, *181*, 3–21.

Ngai, E. W. T., & Wat, F. K. T. (2005). Fuzzy decision support system for risk analysis in e-commerce development. *Decision Support Systems*, *40*(2), 235–255. doi:10.1016/j.dss.2003.12.002

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis*, *31*(3), 497–512. doi:10.1111/j.1539-6924.2010.01478.x PMID:20807381

Ozeir, W. (1988). Risk quantification problems and Bayesian Decision Support System solutions. *Information Age*, *11*(4), 229–234.

Pawlak, Z. (1991). *Rough sets - Theoretical aspects of reasoning about data*. Dordrecht: Kluwer Academic Publishers.

Rakes, T. R., Deane, J. K., & Rees, L. P. (2012). IT security planning under uncertainty for high-impact events. *Omega: International Journal of Management Science*, *40*(1), 79–88. doi:10.1016/j.omega.2011.03.008

Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for Cybersecurity risk planning. *Decision Support Systems*, *51*(3), 493–505. doi:10.1016/j.dss.2011.02.013

Salmela, H. (2008). Analyzing business losses caused by information systems risk: A business process analysis approach. *Journal of Information Technology*, *23*(3), 185–202. doi:10.1057/palgrave.jit.2000122

Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems*, *55*(1), 156–164. doi:10.1016/j.dss.2013.01.001

Shafer, G. (1976). *A mathematical theory of evidence*. Princeton: Princeton University Press.

Smets, P. (1997). Imperfect information: Imprecision - uncertainty, In uncertainty management in information systems: From Needs to Solutions, A. Motro and P. Smets (Eds.), 225-254, Kluwer Academic Publishers, Dordrecht.

Smith, E., & Eloff, J. H. P. (2002). A prototype for assessing information technology risks in health care. *Computers & Security*, *21*(2), 266–284. doi:10.1016/S0167-4048(02)00313-9

Smithson, C., & Paul, S. (2004). Quantifying operational risk. *Risk (Concord, NH)*, *17*(7), 57–59.

Strecker, S., Heise, D., & Frank, U. (2011). RiskM: A multi-perspective modeling method for IT risk assessment. *Information Systems Frontiers*, *13*(4), 595–611. doi:10.1007/s10796-010-9235-3

Tavana, M., Trevisani, D. A., & Clark, T. A. (in press). A Deterministic Risk Analysis and Measurement Model for Assessing Availability and Integrity in Command and Control Systems. *International Journal of Data Analysis Techniques and Strategies*.

Tsai, M.-J., & Wang, C.-S. (2008). A computing coordination based fuzzy group decision-making (CC-FGDM) for web service oriented architecture. *Expert Systems with Applications*, *34*(4), 2921–2936. doi:10.1016/j.eswa.2007.05.017

Viduto, V., Maple, C., Huang, W., & Lopez-Perez, D. (2012). A novel risk assessment and optimization model for a multi-objective network security countermeasure selection problem. *Decision Support Systems*, *53*(3), 599–610. doi:10.1016/j.dss.2012.04.001

Yeh, C. H., & Deng, H. (2004). A practical approach to fuzzy utilities comparison in fuzzy multi-criteria analysis. *International Journal of Approximate Reasoning*, *35*(2), 179–194. doi:10.1016/j.ijar.2003.09.002

Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, *8*(3), 338–353. doi:10.1016/S0019-9958(65)90241-X

Zadeh, L. A. (1978). Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets and Systems*, *1*(1), 3–28. doi:10.1016/0165-0114(78)90029-5

*Madjid Tavana is a professor of Business Systems and Analytics and the Lindback Distinguished Chair of Information Systems and Decision Sciences at La Salle University, where he served as Chairman of the Management Department and Director of the Center for Technology and Management. He is a Distinguished Research Fellow at Kennedy Space Center, Johnson Space Center, Naval Research Laboratory at Stennis Space Center, and Air Force Research Laboratory. He was recently honored with the prestigious Space Act Award by NASA. He holds a MBA, PMIS, and PhD in Management Information Systems and received his Post-Doctoral Diploma in Strategic Information Systems from the Wharton School at the University of Pennsylvania. He is the Editor-in-Chief of Decision Analytics, International Journal of Applied Decision Sciences, International Journal of Management and Decision Making, International Journal of Strategic Decision Sciences, and International Journal of Enterprise Information Systems. He has published several books and over one hundred research papers in academic journals such as Information Sciences, Decision Sciences, Information Systems, Interfaces, Annals of Operations Research, Advances in Space Research, Omega, Information and Management, Knowledge-Based Systems, Expert Systems with Applications, European Journal of Operational Research, Journal of the Operational Research Society, Computers and Operations Research, Energy Economics, Applied Soft Computing, and Energy Policy.*

*Dawn Trevisani is a Program Manager/Computer Scientist with the Decision Support Systems Branch at the Air Force Research Laboratory in Rome, New York. She manages modeling and simulation research, experimentation and analysis programs in response to United States Air Force requirements and documented deficiencies. Her focus has been in the area of Integrated Command and Control (C2) Architectures, Operational Level Resiliency, Decision Support Systems and Course of Action Generation and Assessment. She holds a BS and an MS in Computer and Information Science from State University of New York - Institute of Technology at Utica/Rome. Dawn has published in the International Journal of Information Technology Project Management and International Journal of Data Analysis Techniques and Strategies.*

*Dennis T. Kennedy is an Associate Professor of Business Systems and Analytics at La Salle University. He has a MBA and PhD from Temple University. His research interests include multi-criteria decision making, expert systems, group decision support systems, and distributed consensus building. He has published research in the International Journal of Applied Decision Sciences, International Journal of Information Technology and Decision Making, Business Journal, Benchmarking: An International Journal, Information and Management, Journal of Behavioral Decision Making, Omega, Accounting Enquiries, Journal of Management Systems, Journal of Accounting, Auditing and Finance, and Interface.*

# APPENDIX

## Derivation of the Center Of Gravity for the Trapezoidal Fuzzy Sets

Let $A$ be a fuzzy set defined in $X = \{x_1, ..., x_n\}$ with membership function $\mu_A(x_i)$. Then, the center of gravity of $A$ for the discrete case is defined as follows:

$$cg(A) = \frac{\sum_{i=1}^{n} x_i \mu_A(x_i)}{\sum_{i=1}^{n} \mu_A(x_i)} \tag{A.1}$$

Consider the trapezoidal fuzzy set $A = (a'_{ij}, b'_{ij}, \alpha'_{ij}, \beta'_{ij})$ with a continuous membership function $\mu_A(x)$ defined as follows:

$$\begin{cases} 1 - \dfrac{a'_{ij} - x}{\alpha'_{ij}} & \text{if} \quad a'_{ij} - \alpha'_{ij} \le x \le a'_{ij} \\ 1 & \text{if} \quad a'_{ij} \le x \le b'_{ij} \\ 1 - \dfrac{x - b'_{ij}}{\beta'_{ij}} & \text{if} \quad b'_{ij} \le x \le b'_{ij} + \beta'_{ij} \\ 0 & \text{if} \quad \text{otherwise} \end{cases}$$

Applying the center of gravity Formula (A.1) to the continuous case, we obtain the following expression for the center of gravity of $A = (a'_{ij}, b'_{ij}, \alpha'_{ij}, \beta'_{ij})$:

$$cg(A) = \frac{\int_{a'_{ij}-\alpha'_{ij}}^{a'_{ij}} x\left(1 - \dfrac{(a'_{ij} - x)}{\alpha'_{ij}}\right)dx + \int_{a'_{ij}}^{b'_{ij}} t\,dx + \int_{b'_{ij}}^{b'_{ij}+\beta'_{ij}} x\left(1 - \dfrac{(x - b'_{ij})}{\beta'_{ij}}\right)dx}{\int_{a'_{ij}-\alpha'_{ij}}^{a'_{ij}} \left(1 - \dfrac{(a'_{ij} - x)}{\alpha'_{ij}}\right)dx + \int_{a'_{ij}}^{b'_{ij}} dx + \int_{b'_{ij}}^{b'_{ij}+\beta'_{ij}} \left(1 - \dfrac{(x - b'_{ij})}{\beta'_{ij}}\right)dx} \tag{A.2}$$

Calculating these integral expressions and collecting terms, we find the following formula for $cg(A)$:

$$cg(A) = \frac{a'_{ij}(3a'_{ij} - a'_{ij}) + \beta'_{ij}(\beta'_{ij} + 3b'_{ij}) + 3(b'^2_{ij} - a'^2_{ij})}{3\left[\alpha'_{ij} + \beta'_{ij} + 2(b'_{ij} - a'_{ij})\right]} \tag{A.3}$$