Paper: jc*--**-****

Security Risk Assessment: Towards a Justification for the Security Risk Factor Table Model

Beverly Rivera[1], Francisco Zapata[2], and Vladik Kreinovich[1]

[1]Computational Science Program
[2]Department of Industrial, Manufacturing, and Systems Engineering
University of Texas at El Paso, El Paso, TX 79968, USA
barivera@miners.utep.edu, fazg74@gmail.com, vladik@utep.edu

[Received 00/00/00; accepted 00/00/00]

One of the widely used methods to gauge risk is the Security Risk Factor Table (SRFT) model. While this model has been empirically successful, its use is limited by the fact that its formulas do not have a theoretical explanation – and thus, there is no guarantee that these formulas will work in other situations as well. In this paper, we provide a theoretical explanation for the SFRT formulas.

Keywords: Security risk, SRFT model, statistical justification

1. Formulation of the Problem

Security Risk Factor Table (SRFT) model: a brief description. Many systems face security risks. To properly protect these systems, it is important to gauge relative security risk of different systems, so that more resources will be used to protect systems with higher risk.

One of the widely used techniques for gauging risk is the Security Risk Factor Table (SRFT) model; see, e.g., [2–16, 18]. In this model, important factors affecting risk are listed, such as location, visibility, inventory, etc. For each factor i, experts estimate the risk S_i corresponding to this factor by selecting a number from 0 to 5, 0 meaning lowest risk and 5 meaning highest risk.

Risks S_i corresponding to different factors $i = 1, \ldots, m$ are then added into a single *risk score*

$$S = \sum_{i=1}^{m} S_i.$$

Based on the value of the risk score S, the system's risk is then classified into several categories, e.g., into low, moderate, high, and extreme risk. For that, the experts select thresholds $t_1 < t_2 < \ldots$; then:

- systems with $S < t_1$ are classified as having the lowest possible risk level,
- systems with $t_1 \le S < t_2$ are classified as having the next risk level,
- etc.

Usually, practitioners use four different risk levels: low, medium, high, and extreme. In this case, to separate these four risk levels, we need to select three thresholds t_1, t_2, t_3. Once these three thresholds are selected, we can classify systems as follows:

- systems with $S < t_1$ are classified as low risk;
- systems with $t_1 \le S < t_2$ are classified as medium risk,
- systems with $t_2 \le S < t_3$ are classified as high risk, and
- systems with $S > t_3$ are classified as extreme risk.

The thresholds are usually selected to be *equally spaced*, in the sense the difference $t_j - t_{j-1}$ between each threshold t_j and the previous threshold t_{j-1} is the same for all the thresholds:

$$t_j - t_{j-1} = \text{const},$$

i.e., in other words,

$$t_2 - t_1 = t_3 - t_2 = \ldots$$

For example, for the case when we have $n = 15$ factors, the recommended thresholds are $t_1 = 15$, $t_2 = 30$, and $t_3 = 45$. One can easily check that these thresholds are indeed equally spaced. In this case:

- scores below 15 indicate low risk;
- scores from 16 to 30 indicate moderate risk;
- scores from 31 to 45 indicate high risk, and
- scores above 45 indicate extreme risk.

Related practical and theoretical problems. The SRFT model is empirically successful and widely used. The fact that this model is successful seems to indicate that this model indeed reflects the actual risks.

From the *practical* viewpoint, the key issue in using this model is how to select the appropriate factors and how to determine the best threshold level. This is not as easy as this may sound at first glance, since usually, there are

many possible factors, and selecting the most important ones is a difficult task requiring good expertise in the corresponding area. Not surprisingly, many of the papers that we cite use the words like "expert", "intelligent", "fuzzy", etc., either in the paper titles or in the titles of the journals where they were published.

Once the appropriate factors and thresholds have been selected, the above model usually works very well. This empirical success of the above mathematically simple model raises an important *theoretical* question: why is this model properly reflecting actual risks? Specifically, why adding the scores makes sense? Why equally spaces thresholds – such as $t_1 = 15$, $t_2 = 30$, and $t_3 = 45$ – make sense?

What we do in this paper. In this paper, we analyze the above theoretical challenge. Specifically, we analyze the risk situation, and we show that this analysis indeed explains the two main features of the SRFT model:

- addition of scores $S = \sum_{i=1}^{m} S_i$, and
- equal spacing of thresholds $t_j - t_{j-1} = \text{const}$.

2. Why Adding Scores Make Sense: Our Explanation

A natural way to gauge risk. A natural way to gauge risk for a system is to estimate the expected value of the loss due to a possible attack on this system. In general, the expected loss E is equal to the product $E = P \cdot L$ of the probability P of a successful attack and a loss L caused by this attack.

The success of an attack depends on several independent factors: for the attack to be successful, the location must be vulnerable to an attack, the system must be highly visible, perimeter protection must be weak, etc. Since these factors are independent, the probability P of a successful attack is equal to the product $P = P_1 \cdot \ldots \cdot P_n$ of the probabilities $P_1, \ldots, P_n$ corresponding to these factors.

Thus, we conclude that the expected loss E is equal to the product

$$E = P_1 \cdot \ldots \cdot P_n \cdot L, \tag{1}$$

where the values P_i and E describe different factors affecting risk.

Analyzing the resulting formula. Let us show that the formula (1) enables us to explain the addition of scores.

Before we start our explanation, let us note that while from the purely mathematical viewpoint, the value E depends in a similar way on all $n+1$ factors $P_1, \ldots, P_n$, and L, the ranges of possible values of these factors are different:

- most of the factors are probabilities, i.e., numbers whose possible values are between 0 and 1, while
- the numerical value of the loss L is usually much larger than 1.

To make the formula more symmetric, let us replace the *actual* loss L (e.g., measured in dollars) with a *relative* loss $\ell \stackrel{\text{def}}{=} \dfrac{L}{L_{\max}}$, where $L_{\max}$ is the largest possible loss. Depending on the value of the actual loss L, the relative loss ℓ can take values from 0 (when there is no loss at all and $L = 0$) to 1 (when we encounter the largest possible loss $L = L_{\max}$). The resulting product

$$p \stackrel{\text{def}}{=} P_1 \cdot \ldots \cdot P_n \cdot \ell \tag{2}$$

describes the expected value of the relative loss.

The comparison of risk of different systems does not depend on the units used to describe loss:

- a system with the higher value of E will have the higher value of $\ell = \dfrac{E}{L_{\max}}$;
- similarly, a system with the lower value of E will have the lower value of ℓ.

Thus, we can use the formula (2) to gauge risks.

Now that all the possible values of all the factors $P_1, \ldots, P_n$, and ℓ are between 0 and 1, we can denote ℓ by P_{n+1} and get a simplified formula

$$p = \prod_{i=1}^{n+1} P_i. \tag{3}$$

From the usual formula for risk to score addition. In the usual risk formula, the risk measure is equal to the *product* of risk measures corresponding to different factors. We would like to justify the SRFT technique in which we compute the *sum* of the values corresponding to different factors.

It is possible to go from a product to a sum. For example, we can do it by taking the logarithms – since the logarithm of the product is equal to the sum of the logarithms: $\ln(p \cdot q) = \ln(p) + \ln(q)$. It is worth mentioning that taking logarithms his is, in some reasonable sense, the only way to go from products to sum. Specifically, it is known (see, e.g., [1]) that:

- if we have a monotonic function $f(x)$ for which, for all p and q, we have

$$f(p \cdot q) = f(p) + f(q),$$

- then $f(p) = k \cdot \ln(p)$ for some constant k.

Let us therefore apply the logarithms to the expression (3).

The transition to logarithms does not affect our main objective – of selecting a security scheme that leads to the smallest risk. Indeed, the larger p, the larger its logarithm $\ln(p)$. So, to decide which schemes leads to a smaller risk, instead of comparing the values p corresponding to different schemes, we can alternatively compare the logarithms $\ln(p)$.

For the logarithms, the formula (3) leads to

$$\ln(p) = \sum_{i=1}^{n+1} \ln(P_i). \tag{4}$$

If we use this formula, then, to estimate the overall risk $\ln(p)$ of a system, we add the scores $\ln(P_i)$ corresponding to different factors – and this is exactly what is done in the the SRFT technique.

We have therefore explained why the addition of scores makes sense when assessing the overall risk.

Comment. While we explained why the SRFT idea of adding scores makes sense, the scores $\ln(P_i)$ that we use in our explanation are different from the scores used by SRFT. Indeed:

- the SRFT scores are non-negative, while
- for probabilities $P_i < 1$, the logarithms $\ln(P_i)$ are negative.

To come up with non-negative scores, we can use the fact that the comparison between two quantities x_1 and x_2 does not change if we use a different scale for measuring both quantities, i.e., a different starting point and a different measuring unit. For example, a temperature which is large in the Fahrenheit scale is also larger in the Celsius scale. In general, if we use the new scale $y = a \cdot x + b$ with $a > 0$, then $x_1 > x_2$ if and only if $y_1 > y_2$, where $y_i \stackrel{\text{def}}{=} a \cdot x_i + b$.

So, instead of the logarithms $\ln(P_i)$, we can use expressions $S_i = a \cdot \ln(P_i) + b$. Here,

$$\sum_{i=1}^{n+1} S_i = a \cdot \sum_{i=1}^{n+1} \ln(P_i) + (n+1) \cdot b,$$

so minimizing the sum $\sum\limits_{i=1}^{n+1} S_i$ is equivalent to minimizing the expression (4).

Let us select the values a and b in such a way that the resulting scores match the scale used in the SRFT mode. In SRFT, for each factor i, the worst risk has a score $S_i = 5$, while the smallest risk corresponds to $S_i = 0$. In terms of the corresponding probability P_i, the worst case is when $P_i = 1$, and the best case is when P_i is equal to some predefined small value p_0. (In real life, there is always some risk, so we cannot reach $P_i = 0$.) Thus, we should have $a \cdot \ln(1) + b = 5$ and $a \cdot \ln(p_0) + b = 0$. The first equality implies $b = 5$, and thus, the second leads to $a \cdot \ln(p_0) = -b = -5$ and $a = \dfrac{5}{|\ln(p_0)|}$. So, we should use the values

$$a = \frac{5}{|\ln(p_0)|} \text{ and } b = 5.$$

3. Why Thresholds Are Equally Spaced: Our Explanation

Main idea: let us take into account that risks can be only estimated with some uncertainty. Based on the scores $S_i = a \cdot \ln(P_i) + b$ corresponding to different factors i, we form the summary score

$$S = \sum_{i=1}^{n+1} S_i = a \cdot \ln(p) + (n+1) \cdot b. \tag{5}$$

Since the probabilities P_i (and thus, the scores $S_i = a \cdot \ln(P_i) + b$) are only approximately known, the resulting score is estimated with some estimation error. If the difference between the scores of two different arrangements is smaller than this estimation error, we may not be able to notice this difference based on the estimates corresponding to these arrangements.

Instead of the numerical values of the risk scores – whose exact values are affected by estimation errors – it thus makes sense to consider groups of distinguishable risks.

From the main idea to the actual classification of risks. Based on our estimates for the probabilities P_i, we can estimate the resulting risk p only with some uncertainty. Let us denote the relative accuracy of estimating p by k.

This means that when we know the estimate $\widetilde{p}$ for the relative loss, the actual (unknown) value p of this relative loss can take any value:

- from $\widetilde{p} - k \cdot \widetilde{p}$ (which corresponds to negative estimation error $-k \cdot \widetilde{p}$ of relative size k)
- to $\widetilde{p} + k \cdot \widetilde{p}$ (which corresponds to positive estimation error $-k \cdot \widetilde{p}$ of relative size k).

In other words, the actual value p can be anywhere within the interval

$$[\widetilde{p} - k \cdot \widetilde{p}, \widetilde{p} + k \cdot \widetilde{p}],$$

i.e., within the interval $[\widetilde{p} \cdot (1-k), \widetilde{p} \cdot (1+k)]$.

When the two estimates $\widetilde{p} < \widetilde{q}$ are close to each other, the corresponding intervals

$$[\widetilde{p} \cdot (1-k), \widetilde{p} \cdot (1+k)]$$

and

$$[\widetilde{q} \cdot (1-k), \widetilde{q} \cdot (1+k)]$$

have a non-empty intersection, which means that it is possible that both estimates correspond to the same value of the actual risk p.

The estimates are guaranteed to correspond to different values of risk if the corresponding intervals do not intersect, i.e., when $\widetilde{p} \cdot (1+k) < \widetilde{q} \cdot (1-k)$, or, equivalently, when $\widetilde{q} > \widetilde{p} \cdot \dfrac{1+k}{1-k}$.

For a given $\widetilde{p}$, the smallest value $\widetilde{q}$ which satisfy this inequality – i.e., which correspond to a definitely higher actual risk – is equal to $\widetilde{q} = \widetilde{p} \cdot \dfrac{1+k}{1-k}$. Thus, if we select $\widetilde{p}$ as a representative of a certain level of risk, then the next higher level of risk starts at $\widetilde{q} = \widetilde{p} \cdot \dfrac{1+k}{1-k}$.

Let us start with the value $\widetilde{p}_0$ corresponding to the smallest level of risk. This means that all the values from

the interval $[\widetilde{p}_0\cdot(1-k),\widetilde{p}_0\cdot(1+k)]$ are classified as having the same level of risk as the value $\widetilde{p}_0$, i.e., as having the smallest level of risk.

In accordance with our result, this means that the next level of risk should correspond to the value

$$\widetilde{p}_1=\widetilde{p}_0\cdot\frac{1+k}{1-k}.$$

This implies that all the values $\widetilde{p}$ from the interval

$$[\widetilde{p}_1\cdot(1-k),\widetilde{p}_1\cdot(1+k)]$$

are classified as having the same level of risk as the value $\widetilde{p}_1$. Because of our choice of $\widetilde{p}_1$, the left end $\widetilde{p}_1\cdot(1-k)$ of this interval is equal to

$$\widetilde{p}_0\cdot\frac{1+k}{1-k}\cdot(1-k)=\widetilde{p}_0\cdot(1+k),$$

i.e., to the right end of the interval

$$[\widetilde{p}_0\cdot(1-k),\widetilde{p}_0\cdot(1+k)]$$

describing the previous risk level. Thus, this borderline value

$$T_1=\widetilde{p}_0\cdot\frac{1+k}{1-k}\cdot(1-k)$$

serves as a threshold separating the two risk levels:

- values $p<T_1$ are classified as having the same risk level as the value $\widetilde{p}_0$, i.e., the lowest risk level, while
- value $p>T_1$ are classified as having the same risk level as the values $\widetilde{p}_1$, i.e., the next risk level.

The next interval corresponds to the value

$$\widetilde{p}_2=\widetilde{p}_1\cdot\frac{1+k}{1-k}=\widetilde{p}_0\cdot\left(\frac{1+k}{1-k}\right)^2.$$

The left end $\widetilde{p}_2\cdot(1-k)$ of the corresponding interval

$$[\widetilde{p}_2\cdot(1-k),\widetilde{p}_2\cdot(1+k)]$$

is equal to the right end $\widetilde{p}_1\cdot(1+k)$ of the previous interval

$$[\widetilde{p}_1\cdot(1-k),\widetilde{p}_1\cdot(1+k)].$$

Thus, this common endpoint serves as a threshold

$$T_2=\widetilde{p}_2\cdot(1-k)=\widetilde{p}_0\cdot\left(\frac{1+k}{1-k}\right)^2\cdot(1-k)$$

separating risk levels corresponding to the value $\widetilde{p}_1$ and to the value $\widetilde{p}_2$.

In general, we have $\widetilde{p}_j=\widetilde{p}_0\cdot\left(\frac{1+k}{1-k}\right)^j$. The left end $\widetilde{p}_j\cdot(1-k)$ of the corresponding interval

$$[\widetilde{p}_j\cdot(1-k),\widetilde{p}_j\cdot(1+k)]$$

is also equal to the right end $\widetilde{p}_{j-1}\cdot(1+k)$ of the previous interval

$$[\widetilde{p}_{j-1}\cdot(1-k),\widetilde{p}_{j-1}\cdot(1+k)].$$

Thus, this common endpoint serves as a threshold

$$T_j=\widetilde{p}_j\cdot(1-k)=\widetilde{p}_0\cdot\left(\frac{1+k}{1-k}\right)^j\cdot(1-k)$$

separating risk levels corresponding to the value $\widetilde{p}_{j-1}$ and to the value $\widetilde{p}_j$.

Resulting explanation. For these threshold T_j of relative loss, the corresponding values of risk

$$t_j=a\cdot\ln(T_j)+(n-1)\cdot b$$

take the form

$$t_j=a\cdot\ln(\widetilde{p}_0)+j\cdot a\cdot\ln\left(\frac{1+k}{1-k}\right)+$$
$$a\cdot\ln(1-k)+(n-1)\cdot b. \qquad (6)$$

We can see that these values linearly depend on j, i.e., that they are indeed equally spaced: the difference t_j-t_{j-1} between the two consecutive thresholds t_j is a constant $a\cdot\ln\left(\frac{1+k}{1-k}\right)$ that does not depend on j:

$$t_j-t_{j-1}=\text{const}=a\cdot\ln\left(\frac{1+k}{1-k}\right).$$

We have therefore explained why in the SRFT model, thresholds t_j are equally spaced.

Acknowledgements

This work was supported in part by the El Paso Regional Cyber and Energy Security Center RCES and by National Science Foundation grants HRD-0734825 and HRD-1242122 (Cyber-ShARE Center of Excellence) and DUE-0926721.

The authors are greatly thankful to the anonymous referees for valuable suggestions.

References:

[1] J. Aczél and J. Dhombres, *Functional Equations in Several Variables*, Cambridge University Press, Cambridge, UK, 2008.

[2] Advanced Chemical Safety, Assessing Risk, available at http://chemical-safety.com/documents/pdf/SECURITY

[3] I. Akgun, A. Kandakoglu, and A. F. Ozok, "Fuzzy integrated vulnerability assessment model for critical facilities in combating the terrorism", *Expert Systems with Applications*, 2010, Vol. 37, No. 5, pp. 3561–3573.

[4] American Petroleum Institute (API), *Secirity Guidelines for the Petroleum Industry*, Washington, DC, 2003, available at http://new.api.org/policy/otherissues/upload/Security.pdf

[5] F. Aras, E. Karakas, and Y. Biçen, "Fuzzy logic-based user interface design for risk assessment considering human factor: A case study for high-voltage cell", *Safety Science*, 2014, Vol. 70, pp. 387–396.

[6] R. Arikan, M. Dagdeviren, and M. Kurt, "A Fuzzy Multi-Attribute Decision Making Model for Strategic Risk Assessment", *International Journal of Computational Intelligence Systems*, 2013, Vol. 6, No. 3, pp. 487–502.

[7] L. Atymtayeva, A. Akzhalova, and K. Kozhakhmet, "Main Issues of the Software Development for Knowledge Base Processing in the Intelligent Applications for Information Security Audit", In: J. Musić (ed.), *Recent Advances in Computer Engineering, Communications and Information Technology*, Proceedings of the 8th World Scientific Engineering Academy and Society (WSEAS) International Conference on Computer Engineering and Applications CEA'14, Tenerife, Spain, January 10–12, 2014, pp. 271–280.

[8] S. Baijal and J. P. Gupta, "Site security for chemical process industries", *Journal of Loss Prevention in the Process Industries*, 2005, Vol. 18, pp. 301–309.
[9] S. Baijal and J. P. Gupta, "Securing oil and gas infrastructure", *Journal of Petroleum Science and Engineering*, 2007, Vol. 55, pp. 174–186.
[10] S. Baijal and J. P. Gupta, "Terror-Proofing Chemical Process Industries", *Process Safety and Environmental Protection*, 2007, Vol. 85, No. 6, pp. 559–565.
[11] S. Bajpai, A. Sachdeva, and J. P. Gupta, "Security risk assessment: Applying the concepts of fuzzy logic", *Journal of Hazardous Materials*, 2010, Vol. 173, No. 1–3, pp. 258–264.
[12] H.-J. Kwak and G.-T. Park, "Image contrast enhancement for intelligent surveillance systems using multi-local histogram transformation", *Journal of Intelligent Manufacturing*, 2014, Vol. 25, pp. 303–318.
[13] J. Liu, L. Martnez, H. Wang, R. M. Rodrguez, and V. Novozhilov, "Computing with Words in Risk Assessment", *International Journal of Computational Intelligence Systems*, 2010, Vol. 3, No. 4, pp. 396–419.
[14] M. Nematigoodarzi and M. Tavakoli, "Fuzzy Assessment of Vital Assets Risk in Oil Industry", *Kuwait Chapter of Arabian Journal of Business and Management Review*, 2014, Vol. 3, No. 12, pp. 295–302.
[15] M. Nematigoodarzi, A. F. Farahani, S. E. Hosseini, and M. Tavakoli, "Phase Assessment of Vital Assets Risk in Oil Industry", *International Journal of Biology, Pharmacy, and Applied Science*, 2015, Vol. 4, No. 4, pp. 1858–1867.
[16] A. Srivastava and J. P. Gupta, "New methodologies for security risk assessment of oil and gas industry", *Process Safety and Environmental Protection*, 2010, Vol. 88, No. 6, pp. 407–412.
[17] N. Uttam and P. Verma, "Development of fuzzy model to integrate the human intuition with lead time estimation", *Proceedings of the Conference on Manufacturing Excellence: Imperative for Emerging Economies*, organized by National Institute of Industrial Engineering (NITIE) and Production and Operations Management Society (POMS), Mumbai, India, December 18–21, 2014.
[18] M. van Staalduinen and F. Khan, "A Barrier Based Methodology to Assess Site Security Risk", *Proceedings of the Society of Petroleum Engineers (SPE) Exploration and Production (E&P) Health, Safety, Security and Environmental Conference–Americas*, Denver, Colorado, USA, March 16–18, 2015.

Name:
Beverly Rivera

Affiliation:
University of Texas at El Paso

Address:
500 W. University, El Paso, TX 79968, USA

Brief Biographical History:
2008- Graduate Student, University of Texas at El Paso

Main Works:
• B. Rivera and O. Kosheleva, "How to Predict the Number of Vulnerabilities in a Software System: A Theoretical Justification for an Empirical Formula", Journal of Uncertain Systems, 2015, Vol. 9, No. 2, pp. 133–138.
• B. Rivera, I. Gallegos, and V. Kreinovich, "How to Assign Weights to Different Factors in Vulnerability Analysis: Towards a Justification of a Heuristic Technique", Mathematical Structures and Modelling, 2014, Vol. 30, pp. 87–98.
• R. Martinez, S. Cordero, E. Obregon, I. Gallegos, B. Rivera, et al. "System, Method and Apparatus for Assessing a Risk of One or More Assets Within an Operational Technology Infrastructure", US Patent 20140137257 A1

Name:
Francisco Zapata

Affiliation:
University of Texas at El Paso

Address:
500 W. University, El Paso, TX 79968, USA

Brief Biographical History:
2008- Graduate Student, University of Texas at El Paso
2012- Lecturer, University of Texas at El Paso
2013- Research Assistant Professor, University of Texas at El Paso

Main Works:
• F. Zapata and V. Kreinovich, "Possible Geometric Explanations for Basic Empirical Dependencies of Systems Engineering", Journal of Uncertain Systems, 2015, Vol. 9, No. 2, pp. 151–155.
• F. Zapata, "Partial Orders for Representing Uncertainty, Causality, and Decision Making: General Properties, Operations, and Algorithms", Lambert Academic Publishing, Saarbrücken, Germany, 2013
• F. Zapata, R. Pineda, and M. Ceberio, "How to Generate Worst-Case Scenarios When Testing Already Deployed Systems Against Unexpected Situations", Proceedings of the Joint World Congress of the International Fuzzy Systems Association and Annual Conference of the North American Fuzzy Information Processing Society IFSA/NAFIPS'2013, Edmonton, Canada, June 24-28, 2013, pp. 617-622.

Membership in Learned Societies:
• International Council on Systems Engineering
• Sigma Xi

Name:
Vladik Kreinovich

Affiliation:
University of Texas at El Paso

Address:
500 W. University, El Paso, TX 79968, USA

Brief Biographical History:
1975- Institute of Mathematics, Soviet Academy of Sciences
1980- Leading Researcher, National Institute for Electrical Measuring Instruments, Russia
1989- Visiting Researcher, Stanford University
1990- Professor, University of Texas at El Paso

Main Works:
• H. T. Nguyen, V. Kreinovich, B. Wu, and G. Xiang, "Computing Statistics under Interval and Fuzzy Uncertainty", Springer Verlag, Berlin, Heidelberg, 2012.
• M. Ceberio and V. Kreinovich (Eds.), "Constraint Programming and Decision Making", Springer Verlag, Berlin, Heidelberg, 2014.
• C. Hu, R. B. Kearfott, A. de Korvin, and V. Kreinovich (Eds.), "Knowledge Processing with Interval and Soft Computing", Springer Verlag, London, 2008.
• W. Pedrycz, A. Skowron, and V. Kreinovich (Eds.), "Handbook on Granular Computing", Wiley, Chichester, UK, 2008.

Membership in Learned Societies:
• Association for Computing Machinery (ACM)
• Institute for Electrical and Electronic Engineers (IEEE)
• American Mathematical Society (AMS)