Jerzy MIKULIK

Department of Management Engineering , Faculty of Management, AGH University of Science and Technology in Krakow

The impact of disturbed input data sets on the accuracy of mathematical modelling of intelligent building security

Abstract. *The paper presents a project of a method of intelligent building security assessment using the methodology of security modelling in case of incomplete data. Using an appropriate matrix model together with zonal diversification and fuzzy logic, after gathering information on the facility it is possible to identify in the building zones that require special supervision. By identifying these areas, it becomes possible to continue the building modernization in terms of improving safety of its users. However, we often deal with incompleteness, i.e. insufficiency or uncertainty of information collected, which, when used in the calculation model, can cause some divergences. This paper presents the results of studies on selected types of data disturbances and their impact on the results of calculations of the mathematical modelling of intelligent building security.*

Streszczenie. *Artykuł przedstawia projekt metody oceny bezpieczeństwa inteligentnego budynku, przy zastosowaniu metodyki modelowania bezpieczeństwa w warunkach niekompletności danych. Wykorzystując odpowiedni model macierzowy wraz z dywersyfikacją strefową oraz logikę rozmytą można, po zebraniu informacji o obiekcie wskazać strefy budynku wymagające specjalnego nadzoru. Dzięki identyfikacji tych stref możliwa staje się dalsza modernizacja obiektu pod kątem poprawy bezpieczeństwa podczas użytkowania budynku. Jednakże często ma się do czynienia z niekompletnością, czyli niepełnością lub niepewnością zgromadzonych informacji, których zastosowanie w modelu obliczeniowym może wprowadzić pewne rozbieżności. Niniejsza praca przedstawia wyniki badań nad wybranymi rodzajami zaburzeń danych oraz ich wpływem na rezultaty obliczeń modelowania matematycznego bezpieczeństwa inteligentnego budynku. (**Wpływ zaburzonych danych wejściowych na dokladność matematycznego modelowania bezpieczeństwa budynku inteligentnego**)*

Keywords: intelligent building, mathematical modelling of building security, data incompleteness.
Słowa kluczowe: budynek inteligentny, modelowanie matematyczne bezpieczeństwa budynku, niekompletność danych.

Introduction

Buildings affect in different ways people and the environment in which they are located. Nowadays, it is unacceptable to consider a building in isolation from its impact on the environment. The so-called sustainable intelligent buildings are becoming increasingly important. They are characterized by low levels of pollution generated, optimal consumption of electricity and water, integration of all systems of automatic control and a high level of security for users [3, 4, 5, 23].

Intelligent building security assessment concerns professional activities, which are based on sound knowledge, professional skills, sound methods, as well as efficient and effective procedures. All these requirements are essential in case of intelligent buildings, where the multiplicity and the importance of factors affecting security makes comprehensive assessment of the building as a complex system extremely complicated [7,12,13,17,18].

Public buildings, dominant in the group of intelligent buildings, are structures, for which safety is the key factor having impact on their smooth functioning in any conditions. Recently, a strong need has been identified to address seriously the issue of security of these buildings, mainly because of the emergence of new threats associated with terrorism [9]. Their level of complexity, the multiplicity of subsystems operating in them, and consequently, the problem of management connected with many factors influencing decision-making cause that research on the impact of disturbances in the flow of information to the decision-making centre, where decisions on measures to be implemented in dealing with critical situations are taken, have become increasingly important and requisite [16, 20]. Hence, this paper shows the need for developing a comprehensive approach to the security of the system of intelligent building in view of problems with the collection of data required for taking decisions in relation to maintaining security [14].

Many of the requirements are extremely significant in case of important structures, such as utility buildings, in which the multitude and the importance of factors affecting safety make comprehensive assessment of technical security of a complex system exceedingly complicated. The level of complexity of the problem increases significantly especially in situations where empirical data collected in an inspected building in order to use it for further calculations, demonstrates some deficiencies, inaccuracies, is affected by errors or, if, for various reasons, it is impossible to collect all information required by the approved scheme of calculations. Then we have to deal with the problem of inference based on inaccurate information [1, 2, 21].

Articles on the mathematical modelling of technical systems in buildings occasionally appear in the literature [10], but the majority of publications deal with mathematical modelling only of selected security systems [11,15,19]. There are virtually no papers concerning the mathematical modelling of the entire building from the perspective of personal security.

This article presents some guidelines for the assessment of threats occurring in a building in case of disturbances of collected and processed information as well as a method of their analysis and use, which will allow for diagnosing the threats affecting the overall security level of intelligent building and its users.

Data disturbances

Methods of logical inference are unfailing in terms of the accuracy of conclusions reached provided the use of a correct inference system and a certain degree of reliability of information collected and processed. However, in this case, it is necessary to assume that the data contained in the database used is actually considered true. Provided the accuracy of such data, conclusions drawn as a result of the implemented inference procedure are also reliable. Nevertheless, the assumption of unwavering accuracy of collected data often cannot be met in relation to information held by human beings. Man creates the initial contents of a database. Knowledge derived from a human being may be imperfect, especially when it comes from measuring instruments burdened with processing errors, or when it is passed by a larger number of intermediaries, or is subjected to pre-treatment before it is saved in the database. This type of data sets can be presented, for instance, in the form of fuzzy sets [22]:

(1)
$$A = \{(x, \mu_A(x)) \mid x \in X\}$$
$$\mu_A : X \to [0,1]$$

When we deal with disturbed data, using methods that assume accurate knowledge can result in obtaining conclusions, which need not be true, and the accuracy of which cannot be confirmed.

When we take a closer look at the nature of imperfections of gathered information, we can indicate at least three basic types thereof:

- uncertainty of information, which means that some of the collected data is incorrect,
- incompleteness of information, meaning that among the collected data some reliable data required for further processing is missing, however, it is not possible to assume a priori that it is true or false,
- inaccuracy of information in the sense that some of the data collected is burdened with error and therefore it is impossible to determine unambiguously whether it is true or false, or what are some of the relations between the data.

Hence, some methods are needed for characterizing the degree of conviction in the veracity of statements belonging to the initial database. However, if this is not feasible, it may be required to assume the truthfulness or falsehood of certain data in order to conduct inference, but allowing for the possibility to investigate a larger number of cases in the event discrepancies appear in the course of further logical inference. Therefore, it becomes expedient to equip systems performing inference based on imperfect information with special mechanisms for its processing, by which it will be possible to characterize the type and degree of imperfection of information originating from man.

An example of this type of inference mechanism can be Dempster-Shafer theory (TDS) [1], also called the theory of functions of beliefs or mathematical theory of evidence. It can be treated as an extension of the probability theory where event space subsets are assigned a Basic Probability Assignment, for example, *m.* Measure *m* need not be specified on all elements of the event space, and on this measure the conditions are imposed:

(2)
$$m(\varnothing) = 0$$
$$\sum_{A \subseteq 0} m(A) = 1$$

TDS theory is one of the well-known theoretical models of data imperfections, dealing with the adoption of many values of one attribute at the same time. It demonstrates one of the methods of using mathematical probability with subjective assessment.

New dimensions are defined, the so-called belief function (3),

(3)
$$Bel(A) = \sum_{B \subseteq A} m(B)$$

where: *Bel:* $2^{\Theta} \to [0,1]$.

And the plausibility function (4) Pl: $2^{\Theta} \to [0,1]$ such, that:

(4)
$$PI(A) = \sum_{A \cap B \neq 0} m(B)$$

A new range is created [Bel (X), Pl (X)], which becomes a conviction range for information about the X elements, and it corresponds to the value of information on veracity of the thesis under consideration, e.g. concerning the symptoms of a given threat to the security of a room in a building.

According to the used terminology, we shall deal with the so-called discriminating frame Θ, which may be a set of all possible threats for the selected room in the building. TDS theory gives the possibility to combine the descriptions of uncertainty into a new belief function.

Let Θ be the discriminating frame, while *m1* and *m2* are the basic probability assignments on Θ, then *m1 ⊕ m2* is a function *m1 ⊕ m2* : $2^{\Theta} \to [0,1]$ such that:

(5)
$$\mathrm{m}_1 \oplus \mathrm{m}_2(\varnothing) = 0$$
$$m_1 \oplus m_2(C) = \frac{\sum\limits_{A \cap B = C} m_1(A) * m_2(B)}{1 - \sum\limits_{A \cap B = \varnothing} m_1(A) * m_2(B)}$$

for all A ⊆ Θ and A ≠ ∅.

For the function defined according to (5) the corresponding belief function is *Bel1⊕Bel2:* $2^{\Theta} \to [0,1]$, such that:

(6)
$$Bel1 \oplus Bel2(A) = \sum_{B \subseteq A} m_1 \oplus m_2(A)$$

Computation model with uncertain information

The method of modelling security discussed in this article entails the necessity to divide building into a finite number of areas. Methodically, a matrix security model has been proposed, consisting of at least two *M x N-dimensional* arrays, here matrices **A** and **P,** for the *K* selected variables that will describe the major types of threats for rooms in the building. These variables can be either deterministic or stochastic.

Matrix $\mathbf{A}_k$ for the selected k threat should be filled according to the formula:

(7) $\mathbf{A}_k = [\, a_{ij} \,]_k$, i=1,2,...M, j=1,2,...N, k=1,2....K

where : *M* is the number of areas, *N* – is the number of zones (e.g. floors in a building), *K* – is the number of threats.

The cells of the matrix $[\, a_{ij}]_k$ represent imprecise, uncertain or incomplete information on the impact of the examined threat on the selected room in the building. These data are collected in numerical form or by using linguistic variables, and then are standardized to the normalized range [0.0 - 1.0].

Selected zones may overlap with a physical, intuitive division of the structure, such as floors in the building. They may also constitute a kind of discontinuous distribution, for instance groups of rooms located in the building and having the same utility. The division can also be purely virtual and dynamically changing. Zoning can also be done into areas facing a similar type of threat.

Matrix $\mathbf{A}_k$ shown symbolically as another layer in Figure 1 describes a method of the division of the building into areas based on a specific type of threat. Matrix A_k has dimension M x N, where M is, for example, the number of analyzed rooms on the floor, and N may indicate the number of floors in the building. The cells of the matrix A_k represent uncertain, incomplete or imprecise data in standardized colour scale. A cell of matrix $\mathbf{A}_k$ with a value ranging between [0.9-1.0] denotes reliable data, and e.g. a cell with a value ranging [0.15-0.3] data of minor significance. One layer in Fig.1 corresponds to one type of threat.

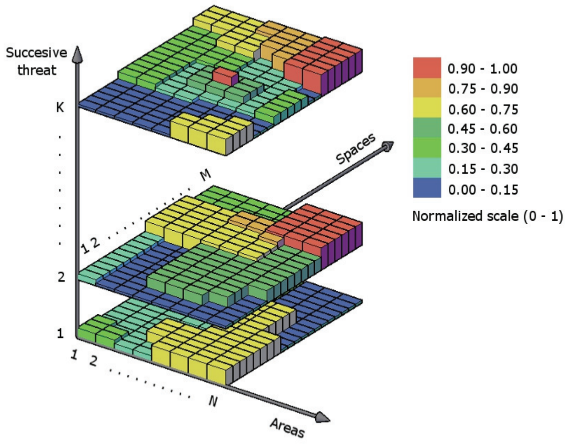


Fig. 1. Visualization of matrix A of vulnerable areas in building for a number (K) types of threat, source: own study

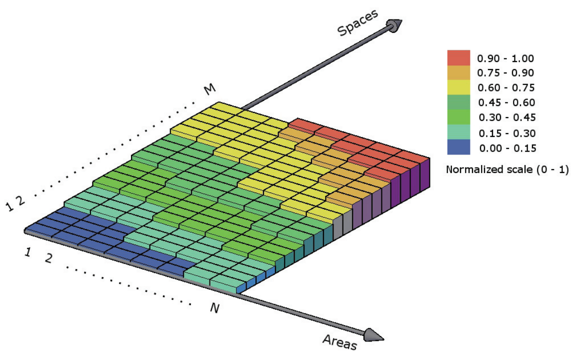


Figure 2.Visualization of matrix $\mathbf{P_k}$ as significance matrix for *k* identified threats in the building, source: own study

Subsequently, the second *MxN-dimensional* matrix $\mathbf{P_k}$, the so-called significance matrix, is defined. It qualifies the degree of impact on the building security of each of *K* threats selected for the analysis. The cells of the matrix $\mathbf{P_k}$ represent the importance of the degree of hazard posed by a given threat for the previously selected and described safety zones, Fig.2. The cells of the matrix P_k demonstrate in a standardized, colour scale the relevance of the analyzed threat for each room in the building. A colour cell of the matrix P_k with values ranging between [0.9-1.0] denotes the highest degree of threat for a room in the building. Similarly, for example, a colour cell with the value in the range [0-0.15] means the insignificance of a given threat.

Filling the matrix P_k follows the equation:

(8) $[p_{ij}]_k = b_l(i,j)$ *dla* $i=1,2,...M,\ j=1,2...N,\ l=1,2,...K$

Values of the $b_l(i,j)$ parameter in the mutual comparison for different *l* variables should reflect the degree of impact of each variable on the overall security level. In other words, the values of $b_l(i,j)$ determine how dangerous is the threat with the number *l* for the $[a_{ij}]_k$. cell of the matrix. Therefore, the $b_l(i,j)$ values should be defined as correlation between the hazard associated with *l* factor and observations, measurements or statistics collected as linguistic data from the entire facility.

The next steps of the construction of the mathematical model involve normalization of the aforementioned two input matrices $\mathbf{A_k}$ and $\mathbf{P_k}$ and calculating the Hadamard product for them according to (9)):

(9) $[a_{ij}]_k \bullet [p_{ij}]_k = [r_{ij}]_k = [a_{ij} \cdot p_{ij}]_k$ dla $i=1,2,...M,\ j=1,2,...N,\ k=1,2,..K$

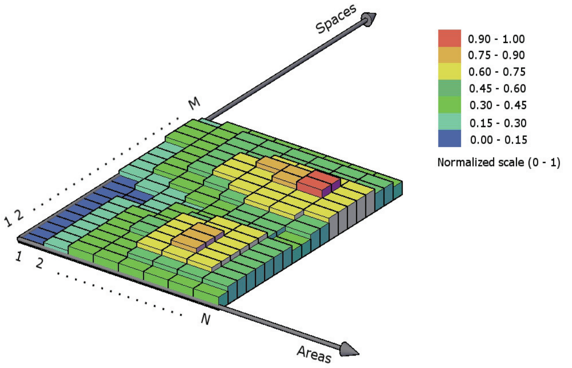


Fig.3. Visualization of matrix $\mathbf{R_k}$ as a result of the influence of the significance matrix $\mathbf{P_k}$ on the matrix $\mathbf{A_k}$ of threatened areas in a building **,** source: own study

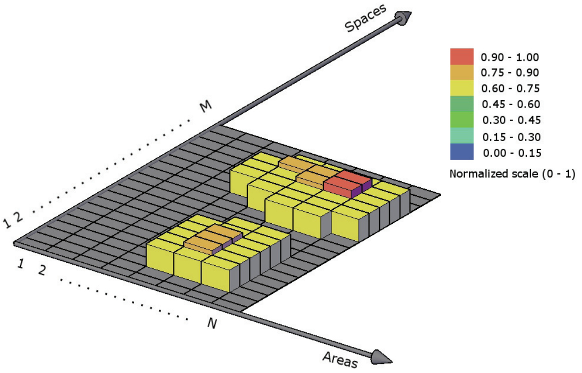


Fig. 4.Visualization of standardized matrix $\mathbf{R_k}$ (for one selected threat) after adjusting the mathematical model, source: own study

Matrix $\mathbf{R_k}$ obtained by computing is the final element needed for the interpretation and analysis of results. The visualization of matrix $\mathbf{R_k}$ shows in general an *MxN-dimensional* layer filled with irregular content in terms of value of individual items. The resulting matrix R_k for one selected threat (in a standardized scale described with colours) is shown in Fig.3.

Subsequently, it is sufficient to carry out appropriate adjustment of the model, which consists in cutting off or resetting in the *MxN-dimensional* matrix (layer) the least significant values, which are below a certain threshold level, in order to obtain as a result an example of its visualization as shown in Fig. 4. Now a cell of the matrix R_k with values from the range [0.9-1.0] denotes the highest level of the analyzed threat for the given room.

It is necessary to note the importance of correct assembly of data for the analysis in the initial phase of the construction of the model. It is worth considering in what ways various types of disturbance of the collected data, as the information on each of the zones, into which the building has been divided, affect the result of calculations. Perhaps, in individual cases, it is possible to notice some regularity, which will allow for the introduction of correction factors at any stage of calculations, or for preliminary processing of the collected data in order to mitigate the potential impact of an adverse factor. It can also turn out that mere observation of the building is sufficient to correct the received data, and thereby to identify a solution adequately close to the valid one, meaning a solution, for which we assume no input data disturbances as well as its full accuracy.

Results of analyses for individual data disturbances

The analysis of inaccurate data is the simplest example of analyzing disturbed input information of the model. Such data may come from measurements made in the zones, into which the building has been divided.

This case only slightly affects the resulting set of areas critical for the building security. At most, values of the model can be disturbed as a result of inaccuracy of data, while, as a rule, the very structure shall remain unchanged. Thanks to this, the areas identified as critical for security will remain unchanged.

In order to define precisely the result of calculations on the matrix model, it is recommended to use correction matrix **D,** taking into account errors of measuring devices.

This matrix assumes unit values for the parameters, which are available from tables or standards; while the remaining matrix values for the parameters measured using measuring devices can take values equal to the inverse of the average relative error of the k_m measuring device. Matrix **D** is built according to the formula:

$$(10) \quad [\, d_{ij} \,] = \begin{cases} 1 - \textit{for standards} \\ \frac{1}{km} - \textit{for measured parameters} \end{cases}$$

i=1,2,…M, j=1,2,…N

The case of inaccurate data shows that the disturbance of inference is insignificant. Any measurement errors in data collection in the tested environment do not affect significantly the results of inference and the identification of critical areas. It often happens that the outcome produced by a model, in which there were data inaccuracies, does not differ from indications of the standard model. The trend of the graph representing the effectiveness of inference is uniform in nature, and the results obtained are satisfactory. Figure 5 depicts the course of inference processes for varying degrees of inaccuracy of data in relation to the standard course (0% inaccurate data is the intermittent curve). Individual waveforms have been obtained for the same overall accuracy of the database, expressed as a percentage, with differences occurring in the accuracy of measurements for each variable.

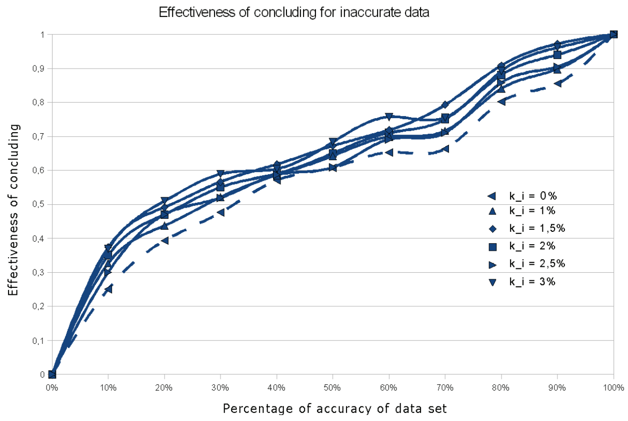


Fig.5. Example of disturbances in the effectiveness of inference for different levels of inaccuracy of input data, source: own study

Figure 6 presents a combination of the visualization of the resulting matrix $\mathbf{R}_k$ obtained for correct input data and the second one - for inaccurate input data. The areas responsible for threat are identified correctly; the only difference concerns the standardized values of cells in relation to the accurate result.

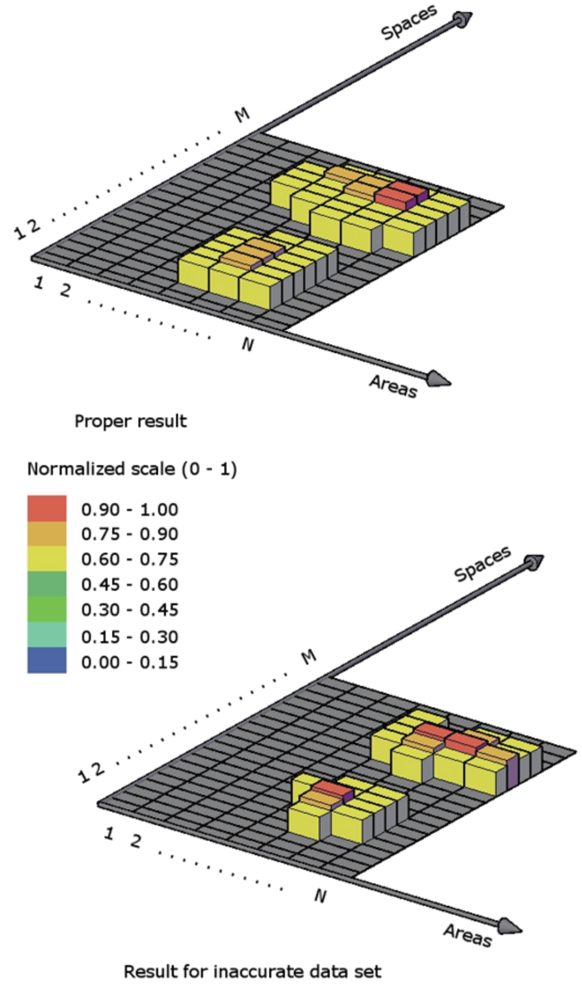


Fig. 6. Example of disturbances of the resulting matrix $\mathbf{R}_k$ for accurate and inaccurate input data, source: own study

In the case of incomplete data, the problem of disturbances of the result in the form of areas critical for the building security is a little bigger. Incompleteness of information means that some data assumed correct has not been collected. The reason for the absence of this information is not important at this point, and the correction of possible defects should be done at the beginning of the process. Sometimes we have to do with a situation, in which data collection is simply impossible (still unknown nature of a phenomenon, damage to the equipment, a very large variability of the tested factor, etc.).

In all such cases, the missing parameters should be estimated by the most competent specialists in the field. In the absence of such persons, based on part of the information collected, distribution of a given characteristic should be estimated as probability distribution.

Then, in case of missing data, the expected value should be assumed, or the missing value should be determined with a certain level of confidence.

The estimator used should be dependent on the number of measurements of a given parameter, which were introduced into the model. In the case of a sample of the size lower than 10, it is reasonable to apply for instance the expected value:

$$(11) \qquad EX = \frac{1}{n}\sum_{i=1}^{n} x_i$$

However, as far as possible, more measurements should be taken, and with their number greater than or equal to 10, standard deviation should be applied as the estimator:

$$(12)\quad 3\sigma = \sqrt{E\left(\left(X - E\left(X\right)\right)^2\right)} = \sqrt{\sum_{i=1}^{n}\left(x_i - \frac{1}{n}\sum_{i=1}^{n}x_i\right)^2}$$

where *E(X)* is the expected value of the random variable *X.*

On the other hand, in situations where the sample of measurement values is characterized by distributions: normal Gaussian (3) or t-Student (4), the properties of these distributions should be used. In such cases we can expect high quality approximations of missing data in the model,

$$(13)\qquad \phi\left(x,\mu,\sigma\right) = \frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

where μ is the expected value, σ – standard deviation.

$$(14)\qquad f\left(t,\nu\right) = \frac{\Gamma(\frac{\nu+1}{2})}{\Gamma\left(\frac{\nu}{2}\right)\sqrt{\nu\pi}}\left(1+\frac{t^2}{\nu}\right)^{-\frac{\nu+1}{2}}$$

where: ν is the number of degrees of freedom of Student's distribution, Γ – Euler's Gamma function

The case of incomplete data (Fig. 7) shows that the disturbance of inference is insignificant. The trend of the graph representing the effectiveness of inference is uniform in nature; however, the results obtained are not reliable to the same degree as in the case of inaccurate data (Fig. 5 and Fig.6). Inference in the presence of data disturbance should not be highly noisy, but in critical cases we can expect a partial or even complete disappearance of critical areas of moderate importance to the level of security of building. Individual waveforms have been obtained for the same general completeness of database, expressed as a percentage, with differences occurring in configurations of deficiencies in individual variables.

The total lack of information in the input data can contribute to the disappearance of values in the significant cells of computing matrix $\mathbf{R_k}$, as depicted in Fig.8. It is a dangerous situation because in the process of computing we lose the protected areas important in terms of building security.

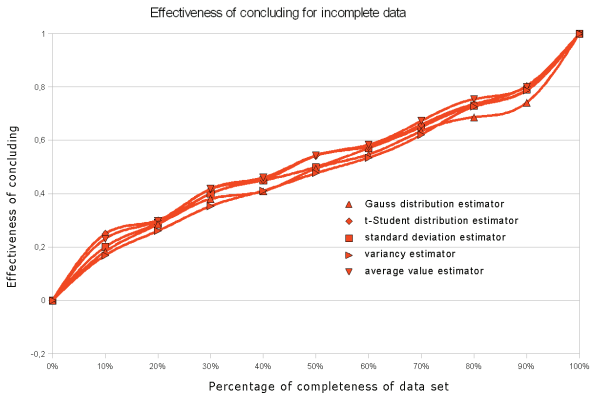


Fig. 7. Example of disorders in the effectiveness of inference for different degrees of data incompleteness, source: own study

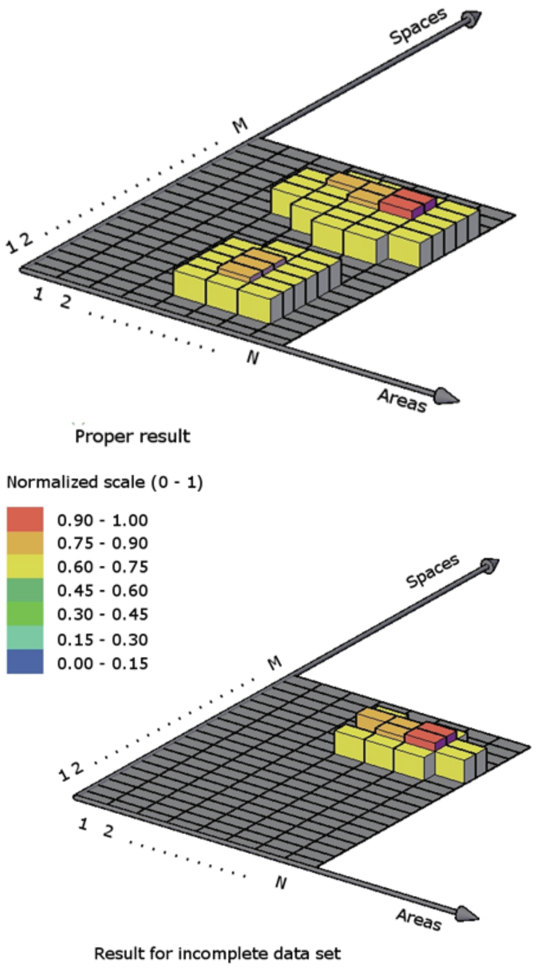


Fig.8. Example of disorders of the result of the matrix method for incomplete data (some areas of the matrix R_k, which should be identified, may disappear due to the lack of input data), source: own study

For this reason at an early stage of calculations it is worth to determine the efficiency of the selected estimator, which can be done by using the Fischer formula (15), [6]:

$$(15)\qquad I(\theta) = E[[\frac{\partial}{\partial\theta}\ln f(X,\theta)]^2]$$

where: *I(θ)* - Fisher information for random variable X for the analyzed parameter θ, f - probability density function, E - mean-square error.

Then the efficiency of the unbiased estimator is defined as:

$$(16)\qquad e(\hat{\theta}) = \frac{\frac{1}{I(\theta)}}{\mathrm{var}(\hat{\theta})}$$

where: $\hat{\theta}$ unbiased estimator of the analyzed parameter *θ*

Please, note that the estimator is called asymptotically unbiased if the bias tends to zero with increasing sample size, which can be formulated as follows:

$$(17)\qquad \lim_{n\to\infty} b(\hat{\theta}) = 0$$

The case of uncertain measurement data and input information is definitely the most difficult one. We have to deal with some false data.

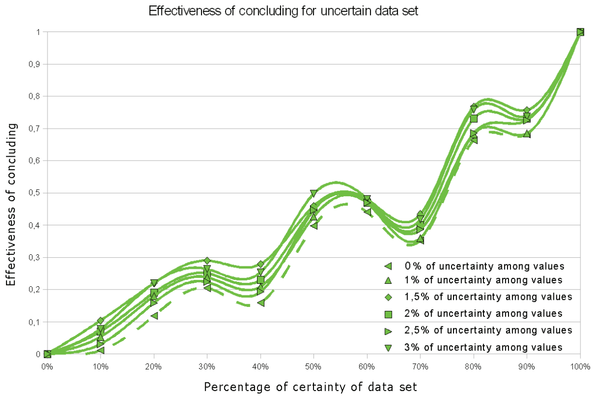
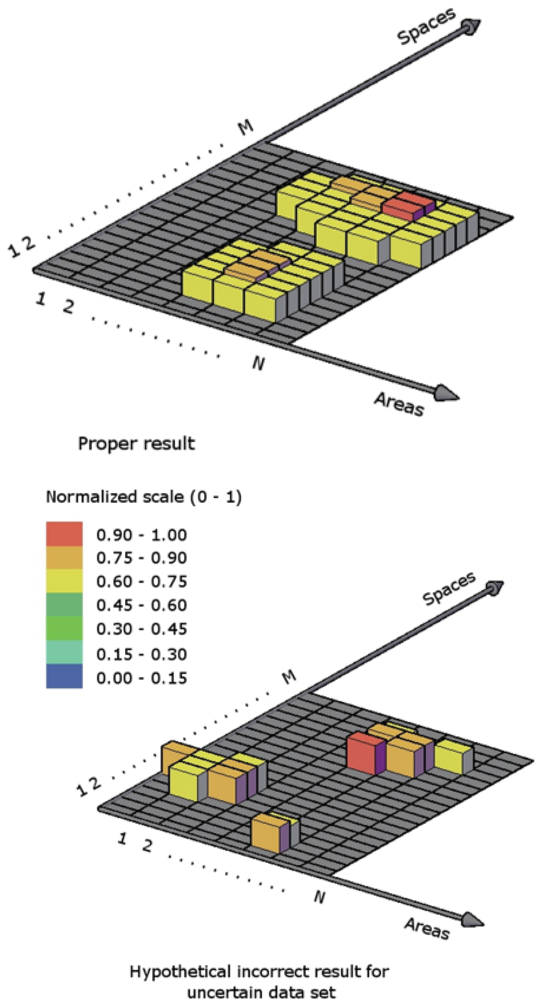


Fig.9. Example of disturbances of inference efficacy for different degrees of uncertainty of data, source: own study



Proper result

Hypothetical incorrect result for uncertain data set

Fig. 10. Example of disorders of the result of the matrix method for uncertain data (additional areas of threat, which in practice are insignificant, appear erroneously in matrix $\mathbf{R}_k$), source: own study

The case of uncertain data shows considerable disorders of the graph trend depicting the efficacy of inference (Fig. 9). The individual waveforms, shown in Fig. 9 have been obtained for the same general uncertainties of the information base, expressed as a percentage, with the differences consisting in the distortion of values for different configurations of variables. The intermittent curve in Fig. 9 depicts the standard course with 0% uncertain data. Depending on which variables are uncertain and how significant they are for the inference process and the result, the disturbance of the result will be higher or lower, but it will always occur in a significant form, and it is difficult to estimate it in such case.

In such a situation, it is impossible to estimate with close approximation the number of uncertain variables, which consequently significantly impedes the error estimation.

REFERENCES

[1] Bolc L. Borodziewicz W., Wójcik M., *Fundamentals of processing uncertain and incomplete information.* Polish Scientific Publishers PWN, Warszawa 1991, (in Polish)

[2] Chromiec J., Strzemieczna E., *Artificial intelligence: methods for design and analysis of expert systems,* PLJ Publishers, Warszawa 1995, (in Polish)

[3] Clements-Croom D., *Intelligent Buildings: design, management and operation,* Thomas Telford, London 2004,

[4] Barry M. Flax - *Intelligent buildings,* IEEE Communications Magazine, Vol.29, April 1991, pp.24-27,

[5] Marion R. Finley, Ancilla Karakura, Raphael Nboni - *Survey of intelligent building concepts,* IEEE Communications Magazine, Vol.29, April 1991, pp.18-23,

[6] Frieden B. R., Gatenby R.A. – *Exploratory data analysis using Fisher information*, Springer-Verlag London, 2007,

[7] Gassmann O, Meixner H - *Sensors in intelligent buildings,* WILEY-VCH Verlag GmbH, 2001,

[8] Haykin S. – *Telecommunication systems*, Telecommunications Publishing House, Warszawa, 2004, (in Polish),

[9] Indecki K. - *Terrorism - practical-dogmatic approach,* WIS Publishing House, Poznań, 2006, (in Polish)

[10] Xiaoshu Lu, Derek Clements-Croom, Martti Viljanen - *Past, present and future mathematical models for buildings: focus on intelligent buildings,* Intelligent Buildings International, Vol.1, No.1, 2009, pp.23-38,

[11] Ren C. Luo, Shin Yao Lin, Kuo L. Su - *A multiagent multisensory based security system for intelligent building,* IEEE Conference on Multisensor Fusion and Integration for Intelligent Systems, 2003, pp.311-316,

[12] Mikulik J.- *Basic security systems in intelligent buildings,* Silesian University of Technology Publishing House, 2005, 2010, (in Polish)

[13] Mikulik J.- *Selected problems of ensuring security and comfort in buildings,* AGH University of Science and Technology Publishing House, Cracow, 2008,

[14] Mikulik J., Zajdel M., *Automatic risk control basing on FSA methodology adaptation for safety assessment in intelligent buildings,* International Journal of Applied Mathematics and Computer Science, Zielona Góra, 2009

[15] Ren C. Luo, Kuo L. Su - *Autonomous fire-detection system using adaptive sensory fusion for intelligent security robot,* IEEE / ASME Transations on mechatronics, Vol.12, No.3, June 2007, pp.274-281,

[16] Ross J.A. - *Security engineering: a guide to building dependable distributed systems,* John Wiley & Sons, 2001,

[17] Ryczer A. *The strategy of intelligent building security management,* Proc 2nd International Congress on Intelligent Building Systems, Text Publishing House, Cracow 2002,

[18] Ryczer A. - *The method of intelligent building security grade assessment,* Proc 5th International Congress on Intelligent Building Systems, Text Publishing House, Cracow, 2010,

[19] Sue Sharples, Vic Callaghan, Graham Clarke - *A multi-agent architecture for intelligent building sensing and control,* International Sensor Review Journal, May 1999, University of Essex,

[20] Stephans R.A., *System Safety for the 21st Century,* Wiley, New Jersey, 2004.

[21] Tarnowski W., *Systems modelling,* Koszalin University of Technology Publishing House, Koszalin 2004, (in Polish),

[22] Tadeusiewicz R. – *Elementary introduction to neural networks techniques with exemplary programs,* Warszawa, Academic Publishing House PLJ, 1998, (in Polish),

[23] J.K.W. Wong, H. Li, S.W. Wang - *Intelligent building research: a review,* Automation In Construction, Vol.14, 20

Author: *dr hab inż. Jerzy Mikulik, prof. AGH, AGH University of Science & Technology in Cracow, Faculty of Management, Department of Management Engineering, 30-067 Krakow, ul.Gramatyka 10, E-mail: jmikulik@zarz.agh.edu.pl*