18(3), pp.327-407, 2020 ISSN 1334-4684

INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS

Scientific Journal

Scientific Journal
INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS

INDECS, volume 18, issue 3, pages 327-407, year 2020
Published 30th September 2020 in Zagreb, Croatia
Released online 30th September 2020

Office

Croatian Interdisciplinary Society
c/o Faculty of Mechanical Engineering & Naval Architecture
I. Lučića 1, HR – 10 000 Zagreb, Croatia
E-mails: editor@indecs.eu (for journal), ured@idd.hr (for publisher)

Editors

Josip Stepanić, Editor-in-Chief, University of Zagreb, Zagreb (HR)
Josip Kasać, Assistant Editor, University of Zagreb, Zagreb (HR)
Mirjana Pejić Bach, Assistant Editor, University of Zagreb, Zagreb (HR)

Advisory Board

Vjekoslav Afrić, University of Zagreb, Zagreb (HR)
Aleksa Bjeliš, University of Zagreb, Zagreb (HR)
Marek Frankowicz, Jagiellonian University, Krakow (PL)
Katalin Martinás, Eötvös Loránd University, Budapest (HU)
Gyula Mester, University of Szeged, Szeged (HU)
Dietmar Meyer, Budapest University of Technology and Economy, Budapest (HU)
Sibila Petlevski, University of Zagreb, Zagreb (HR)
Wei-bin Zhang, Ritsumeikan Asia Pacific University, Beppu (JP)

Editorial Board

Serghey A. Amelkin, Program Systems Institute, Pereslavl-Zalesskij (RU)
Nikša Dubreta, University of Zagreb, Zagreb (HR)
Robert Fabac, University of Zagreb, Varaždin (HR)
Francesco Flammini, Linnæus University, Växjö (SE)
Erik W. Johnston, Arizona State University, Phoenix (US)
Urban Kordeš, University of Ljubljana, Ljubljana (SI)
Dean Korošak, University of Maribor, Maribor (SI)
Anita Lee-Post, University of Kentucky, Lexington (US)
Olga Markič, University of Ljubljana, Ljubljana (SI)
Damir Pajić, University of Zagreb, Zagreb (HR)
Petra Rodik, University of Zagreb, Zagreb (HR)
Armano Srbljinović, University of Zagreb, Zagreb (HR)
Karin Šerman, University of Zagreb, Zagreb (HR)
Karolina Ziembowicz, The Maria Grzegorzewska University, Warszawa (PL)

Technical Editor

Davorka Horvatić, Croatian Interdisciplinary Society (HR)

Published by *Croatian Interdisciplinary Society* (http://www.idd.hr) quarterly as printed (ISSN 1334-4684) and online (ISSN 1334-4676) edition. Printed by *Redak d.o.o.* (HR) in 50 pieces. Online edition, http://indecs.eu, contains freely available full texts of published articles.

Journal INDECS is financially supported by Croatian Ministry of Science and Education.

Content of the journal INDECS is included in the DOAJ, EBSCO, EconLit, ERIH PLUS, Ulrich's and Web of Science Core Collection.

INDECS publishes original, peer-reviewed, scientific contributions prepared as reviews, regular articles and conference papers, brief and preliminary reports and comments to published articles. Manuscripts are automatically processed with the system Comet, see details here: http://journal.sdewes.org/indecs.

The accessibility of all URLs in the texts was checked one week before the publishing date.

TABLE OF CONTENTS

COMPLEX SYSTEMS AND SMART CITIES RESEARCH. EDITORIAL

The present thematic issue of INDECS examines the design and research philosophy of complex systems such as smart cities and the developments related to these technologies.

The urban structures and technological advances presented in this thematic issue support the goals of sustainable development in communities, where these intelligent and smart systems will cover all aspects of life. Some of the topics discussed include, for example, smart city application development, drone localization, smart city solutions, information security management, lightning protection of electric vehicles, cybersecurity, drone systems, safety-critical embedded systems and fiber optical communication system. The relationship between various research topics, and some emerging, sustainable and safe city implementations will also be presented.

The aim of the present thematic issue is to offer researchers an opportunity to extend their existing scientific relationship all over the world in the field of interdisciplinary research in complex systems, such as the field of smart, sustainable and safe cities programmed by NextTechnologies Ltd. Complex Systems Research Institute.

NextTechnologies Ltd. Complex Systems Research Institute was founded in 2019 to provide the framework for our scientific research work on complex systems. In the forthcoming years, this research institute will help organise and further support the Smart, Sustainable and Safe Cities Conference, with the inclusion of the following fields and departments, in particular: Mathematics Division, Informatics Division, Safety and Secutrity Division, Drone Technologies and Drone Applications Division, Intelligent Railway System Division, Robotics / Cooperative Robotics Division and Smart Sustainable Safe Cities Division.

The majority of these studies focus on smart cities, and they can be successfully implemented in various areas of developing sustainable and safe communities all over the world.

Cordially,

Budapest, 5th August 2020

Guest editors

Gyula Mester

Dániel Tokody

Interdisciplinary Description of Complex Systems 18(3), 327-336, 2020

RISK-ADAPTED ACCESS CONTROL WITH MULTIMODAL BIOMETRIC IDENTIFICATION

Gábor Werner[1,] * and László Hanka[2]

[1]Óbuda University, Applied Biometric Institute
Budapest, Hungary

[2]Óbuda University, Institute of Mechatronics and Autotechnics
Budapest, Hungary

DOI: 10.7906/indecs.18.3.1
Regular article

Received: 31 January 2019.
Accepted: 3 March 2020.

ABSTRACT

The presented article examines the background of biometric identification. As a technical method of authentication, biometrics suffers from some limitations. These limitations are due to human nature, because skin, appearance and behavior changes more or less continuously in time. Changing patterns affect quality and always pose a significantly higher risk. This study investigated risk adaption and the integration of the mathematical representation of this risk into the whole authentication process. Several biometrical identification methods have been compared in order to find an algorithm of a multimodal biometric identification process as a possible solution to simultaneously improve the rates of failed acceptations and rejections. This unique solution is based on the Adaptive Neuro-Fuzzy Inference System and the Bayesian Theorem.

KEY WORDS

multimodal biometrics, artificial intelligence, ANFIS, risk management

CLASSIFICATION

ACM: Security and privacy, Biometrics

JEL: Z13

*Corresponding author, η: wga.bme@gmail.com; +36 20 411 8184;
Hungary 1034 Budapest, Bécsi út 96/b

INTRODUCTION

The modern world is surrounded by hidden layers of authentication protocols. Independent from the professional, governmental or private sphere, there is information that has a different value for users. This value sometimes is not objective, therefore, some information may be worthless for some, while others could not live without it. As the amount of personal information and linkages among components are growing, the security behind data management becomes a crucial issue.

In highly secured systems there are strict protocols for access privileges. These protocols involve the use of difficult passwords, multifactor authentication, two key encryption, etc. Nevertheless, there are common attributes in these techniques; they are quite complicated, and it is necessary for all users to know a unique key (password) or to own a hardware (tag) to complete identification.

Biometrics has a history in identification in the field of forensics, rather than in encryption. For instance, the first mobile phone with fingerprint reader on the market was the Toshiba G500 in 2007, but the large-scale spread started with the iPhone 5s in 2012, and nowadays almost all middle class mobile phones are equipped with an inbuilt fingerprint reader, and according to the latest developments the newest generations of smartphones will not have any separate fingerprint readers, instead it is going to be built into the screen [1]. In the mobile market, in addition to the fingerprint reader biometrical technique, face recognition through the front camera, and voice recognition will be used as well. There are also some non direct biometrical traits that can be called personal identification samples, like movements of the user or the way of typing or browsing.

Whether the secured data is personal, official or governmental, the protection highly depends on the users and their skills. Usually a user has to remember several passwords and even correctly recall the correct positions of the letters, numbers or symbols. The user should not share it, lose it or save it onto a public surface. However, the human nature is less likely to be capable of remembering such a multitude of accurate sequences of codes, nor is it precise enough to handle a hardware tool, or it is simply inconvenient to do so.

The biggest challenges of the practical use of applied Biometrics are caused by the limitations above. Biometric identification seems to be more suitable, but it is still not used everywhere. The fact is, biometrics faces some social barriers, data encryption and storage challenges. However, the technical environment took a big step forward, – as it has been shown in the mobile market – as biometric contact is not only used for access control, it is becoming a live interaction between the machine and the user. For instance, in the not too distant future an autonomous car will be able to identify its drivers and even recognize the conditions and intentions of the drivers [2].

REVIEW OF RISK-ADAPTION

ROLE OF RISK

According to Haimes, risk management must be an integral part of decision making. As a system, biometric devices face hazards (malfunction, forced entry, terrorism, etc.) and all these have some consequences. The caused impact can be moral, confidential, financial or technological trauma. If risk management takes a part in the complete system engineering process, it will help to find the balance between the uncertain benefits and costs [3].

From a professional aspect, risk management is a tool which creates the opportunity to find the most suitable solutions and methods. For instance there are several access control techniques (RFID, keypad, biometrics, guard, etc.) that could be used when facing a given problem, but if the system-engineering does not take the real threats and significant

consequences into consideration, the designed access control system might be inefficient or non-cost-effective.

MAIN ELEMENTS OF RISK CALCULATION

In a holistic risk assesment, basically all possible future states have to be taken into account, just like in an event tree analysis, which is a forward logical modeling technique for both success and failure states in the future. There are outcomes that are favorable and those that are not. From the initial state, regarding the circumstances, there is a likelihood of each future situation. Following Bayes' Theorem, each step has an aggregated likelihood from the priori elements, this is called conditional probability. Each element, step and impact has its exact place in the network of happenings. Risk calculation is a method where the significant effects and linkages are explored. In Haimes' terminology there are questions that have to be answered to set up the network [3]:

- What can go wrong?
- What is the likelihood that it would go wrong?
- What are the consequences?

The questions below investigate linkages between networks:

- What can be done and what options are available?
- What are the associated trade-offs in terms of all relevant costs, benefits and risks?
- What are the impacts of current management decisions on future options?

The last question is particularly important, because a poorly chosen management decision can restrain development, especially if the current factor is at the beginning of a sudden rising phase. For example, in the European Union since the Convention on Road Traffic (Vienna, 1968) autonomous cars not allowing human intervention have been banned, so manufacturers must still provide the possibility of human actions to drive.

MODELING RISK ANALYSIS

Risk management cannot be done without measurement and mathematical proceedings. The pareto optimum as an adequate goal of risk management is an intermediate point among the fitted descriptive functions. These function parameters and variables determine the optimum point. But in some cases it is difficult to determine these points, because of the attributions:

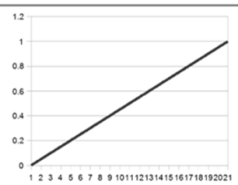	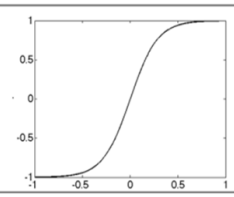	1. Linear vs. non-linear
$a, b, c, \ldots = \alpha, \beta, \gamma, \ldots$ $x, y, z, \ldots = \delta, \theta, \vartheta, \ldots$	$a, b, c, \ldots = P(\alpha), P(\beta), P(\gamma), \ldots$ $x, y, z, \ldots = P(\delta), P(\theta), P(\vartheta), \ldots$	2. Deterministic vs. stochastic
$a, b, c, \ldots = \alpha, \beta, \gamma, \ldots$ $x, y, z, \ldots = \delta, \theta, \vartheta, \ldots$	$a, b, c, \ldots = \alpha(t), \beta(t), \gamma(t), \ldots$ $x, y, z, \ldots = \delta(t), \theta(t), \vartheta(t), \ldots$	3. Static vs. dynamic
$a_i, b_i, c_i \quad i = 1, \ldots, n$	$a_i \quad i = 1$	4. Distributed parameters vs. lumped parameters

Figure 1. Attributions of risk analysis models.

Regarding the distinctive aspects above, different model types can be introduced as the following:

1) A linear model is one that is represented by linear equations. A nonlinear model is represented by nonlinear equations; that is, part or all of the constraints or the objective functions are nonlinear [3].

2) Deterministic models are those in which each variable and parameter can be assigned a definite fixed number or a series of fixed numbers for any given sets of conditions. In probabilistic (stochastic) models, neither the variables nor the parameters used to describe the input-output relationships and the structure of the elements (and the constraints) are precisely known [3].
3) Static models are those that do not explicitly take the variable time into account. Dynamic models are those involving difference or differential equations. Static optimization problems called mathematical programming, while dynamic optimization problems are often referred to as optimal control problems [3].
4) A lumped parameter model does not consider variations, and the various parameters and dependent variables can be considered to be homogeneous throughout the entire system. A distributed parameter model takes into account detailed variations in behavior from point to point throughout the whole system [3].

In Biometrics the background of risk assessment is more complex than the conventional index numbers anticipate. Common quality marks, like the rate of false acceptance (FAR) or false rejection (FRR) are only statistical results. To scientifically prove the compliance, it is necessary to get better involved, for example, by investigating the mathematical and physical model of the entire biometrical identification.

RISK-ADAPTION IN BIOMETRICS

As it is written by Jain et. al., in biometric identification there are several possibilities to cause an error in an authentication systems [4]. To understand the differences, errors must be distinguished. Two main kinds of error sources can be named: intrinsic failures and adversary attacks. An unintentional inner failure is caused by inadequate operation by the biometric device, so a user will be mistakenly rejected or accepted, even though he or she is not an impostor. The other set of errors are adversary attacks, which can aim at administration, the infrastructure or the users directly. In this study administrational and pattern theft from the user is less discussed compared to the direct attacks against the biometric system itself. A compromised system is facing two main threats: the secured objects will not be available to someone/anyone because the system breaks down, or an impostor gains entry into the system. From security aspects, these two sets of outcomes have important differences.

The Denial of Service Attack (DoS attack) as a classic hacking procedure is very similar to the first case. The basic idea in these cases is not about getting sensitive information or data, just merely preventing the operation of the service. For instance, if the operation is locking an access point, then there must be another entrance, or a safety key that could be used as a secondary option. So if there is a risk of DoS attack, the redundancy and the protection of the infrastructural parts becomes more crucial [5].

The other types of malicious actions are hacks. In our interpretation, hacking means a malicious act of an attacker intended to gather information or goods. According to Ratha, there are several points where an attacker can intervene into the biometrical authentication system. Four categories can be named; attacks on the user interface (input stage), attacks on the interface between modules, attacks on the modules, and attacks on the template database [6].

The vulnerability of the stages depend on many circumstances, such as time, preparedness of the attacker, the complexity of the algorithm, the dignity of the manufacturer and the responsible security personnel who applied or run the device. There are eight nominated points where an assault can be provided regarding the entire system of access control [6]:

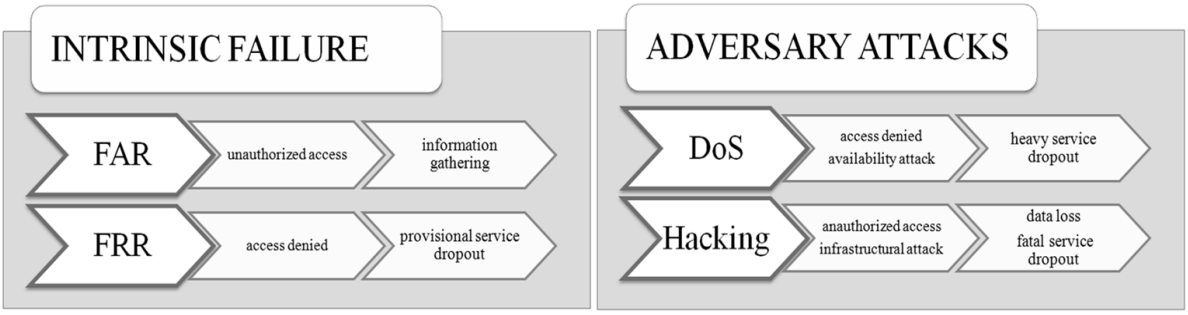

Figure 2. Impact of the errors from different sources.

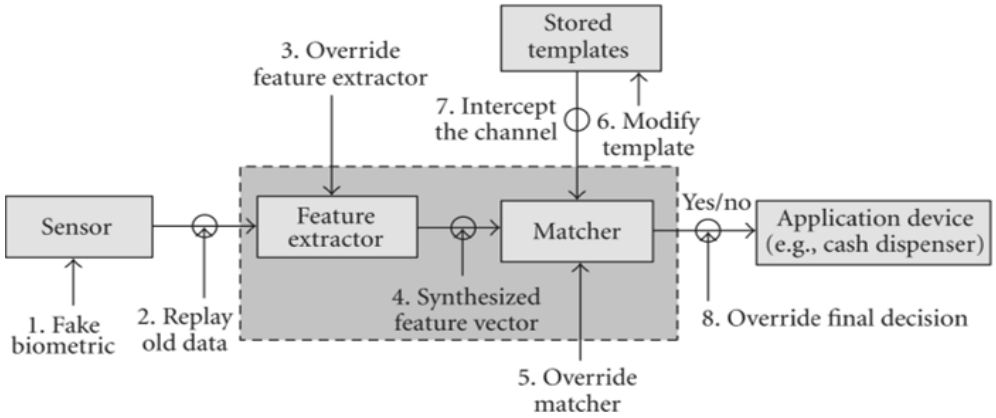

Figure 3. Possible points of attacks in a generic biometric system [6].

RISK MITIGATION POSSIBILITIES IN BIOMETRICS

As it was showed above, an impostor can intervene at several points in a biometric authentication system, including unsecured communication channels, algorithmic loopholes or even the physical design. From practical aspects, the protection of a secured access point (virtual of physical space) is characterized by the complexity of the security system, which should not be more expensive than the protected value, which can also mean reliabilty or personal trust.

In this case the total value approach must be applied, therefore, the complexity of the database management, the total spent time (denied access, error correction, etc.) and the costs of enhanced quality must be taken into consideration collectively. To determine the total cost, both the internal and the external effects have a significant impact, but it can be difficult to recognize and estimate some externalities, such as the social value.

In our case the chain model of the authentication process can be more precisely described by a mathematical model in which the vulnerability points are calculated as a multiplication instead of an addition. This assumption can be confirmed by the Bayes Theorem. Therefore, not only is the logical bond simpler, but also the roles of the attacked points are equal, which allows an easier comparison of different biometrical methods.

According to a study by Srivastava, biometric devices can be compared by many attributions, some of which have a significant role in value-based risk assessment [7].

Where the compared attributes are the following:

- Uniqueness: Each individual should have features but different from the other.
- Permanence: Biometrics should be sufficiently invariant over a certain period of time
- Universality: Population coverage; each individual should have a biometric feature.
- Measurability: Meaning simplicity of extraction and technical equipments..

- Comparability: Simplicity of comparison between templates and the sample.
- Collectability: How well can the identifiers be captured and quantified
- Invasiveness: Introduction of instrument into a body part.
- Performance: Accuracy, speed, security.
- Acceptability: To which extent is it supported by society.
- Circumvention: The act of cheating someone's sample.

Table 1. Comparison of biometric methods [7].

	UNIQUENESS	PERMANENCE	UNIVERSALITY	MEASUREABILITY	COMPARABILITY	COLLECTABILITY	INVASIVENESS	PERFORMANCE	ACCEPTABILITY	CIRCUMVENTION
IRIS	H	H	H	M	M	H	M	H	M	L
RETINA	H	H	H	L	M	M	H	H	L	L
FINGERPRINT	H	H	M	H	M	M	M	M	H	M
PALMPRINT	H	H	M	H	M	M	M	M	H	M
HAND GEOMETRY	M	L	H	H	M	H	M	M	M	M
FACE	M	M	H	M	L	H	L	L	H	H
EAR	M	M	H	M	L	M	L	L	M	L
VOICE	L	L	M	M	L	M	L	L	H	H
KEYSTROKE	L	L	L	L	L	M	M	L	L	M
X-RAYED TEETH	L	L	M	L	L	M	H	L	L	H
SIGNATURE	H	L	L	M	M	H	M	M	H	H
DNA	H	H	H	L	L	L	H	H	H	L

Biometrical identification techniques differ, and they all have their pros and cons, and all techniques have a unique performance depending on the manufacturer. Furthermore, there are several types of algorithms for feature extraction and comparison, so the subset of applicable solutions is even more extensive.

As long as some identification methods theoretically can reach a very low FRR, in practice biometric techniques must face serious obstacles which derive from the extraction process of the biometric sample. This phenomenon can be named as 'noisy interface'. The interface between the human and the machine will be contaminated with some noise in the normal signal. Some devices or the biometric identification methods themselves are sensitive to light, temperature, pollution, fine dirt, etc. These impacts have a high effect on the whole process, because the raw sample will be contaminated, so the distortion will be carried on throughout the whole authentication process. Thus in practical implementations, the environment must be taken into consideration whenever a new biometric device is introduced.

According to our assumption, with a series of data it is possible to statistically estimate the likelihood of the disturbing effects and find a suitable solution for identification.

Nevertheless, in many cases influential external impacts (noises) are not continuous or predictable. Thus if the specific error cannot be minimized, the result will be sensitive to extreme error values, and the FRR increases exponentially.

A good method to decrease the impact of a specific error is to divide it. The distributed specific error method can be implemented in such a situation with parallel multimodal biometric identification. To mitigate some risks, it is necessary to investigate the probability model of the authentication. Basically there are many components that have effects on the cumulated risk. In stochastic models, it is hardly possible to estimate by monitoring the components , the small changes in the user's behavior, environmental effects, etc., so it might be more appropriate to calculate with a multi-cumulated risk value. In order to have two or more cumulated risk values, the method of multimodality must be applied. These values are more discrete, so the summation is easier and there are working models for the calculations.

With regard to the research by John P. Baker at The Johns Hopkins University, it can be stated that the current biometric systems do not meet the performance requirements for high security applications, thus some fusion of multiple biometrics is being considered to help lower error rates. Some biometric systems use all available impressions sequentially until an acceptable match is obtained, while others include logical (AND/OR) operations as a summation of similarity scores. There are more sophisticated methods, that have been considered for combining scores from separate classifiers for each biometric modality using different feature extraction and matching algorithms to generate their scores [8].

METHODOLOGY OF THE MULTIMODAL SUMMATION

John P. Baker proposed a Bayesian belief network (BBN) based architecture for biometric fusion applications. The bayesian networks provide a unified probabilistic framework for optimal information fusion. The Bayesian methods have been used for a long time in biometrics, however the effectiveness and flexibility of the BBN has not been extracted. The networks based on the Bayesian theorem represent the joint probability distribution, where [9]:

$$P(X_1, \dots, X_n) = P(X_n) \prod_{i=1}^{n} P(X_i | parents(X_i)). \quad (1)$$

In the Baker study, the probability can be estimated by the quality, similarly to the study by Ling and Govindaraju. Both use the gamma distribution function, which has been comprehensively investigated in the author's former study about Using the Beta-Binomial Distribution for the Analysis of Biometric Identification [10, 11]. Both studies reveal the importance of two crucial mathematical details, such as the importance of the calculation method of the variables that determine the risk and the method of the fusion or summation of the modalities. Meanwhile the calculation of each modality's likelihood is a more conventional, yet not a simple task, as the fusion and the combined risk of the whole process is more complex.

Our former study found that the failed rejection rate depends on several variables, for which an explicit formula does not exist. As failures come from different subsets of mistakes and statistical uncertainty, the normal binomial fail estimation is not able to lead to the right consequences. For this reason a new 'p' variable has been chosen to the distribution of the probability, instead of a constant. With this methodology it is possible to characterize a biometric device on a smaller sample from a known population [11].

Many solutions have been investigated, but in this article a relatively new method is going to be shown. Human recognition cannot be described as a conventional binary logic, which was stated at first by L. A. Zadeh. Instead of a sharp 'yes' or 'no', the human mind distinguishes on an imaginary line, which Zadeh called the membership function [12].

As a part of soft-computing methods the Fuzzy Logic presents a set of ways of the fusion. Even more so, some variables in the fuzzy sets can be optimized with other soft computing methods, like neural networks or genetic algorithms. These techniques are bringing a new era into risk management with deep learning.

As it has been shown in robotics, the Fuzzy Implication is an appropriate technique for modeling human decisions. According to Takagi and Sugeno, the Fuzzy Implication spread worldwide in control applications and classifiers, and it is also a useful tool for predictions [13, 14].

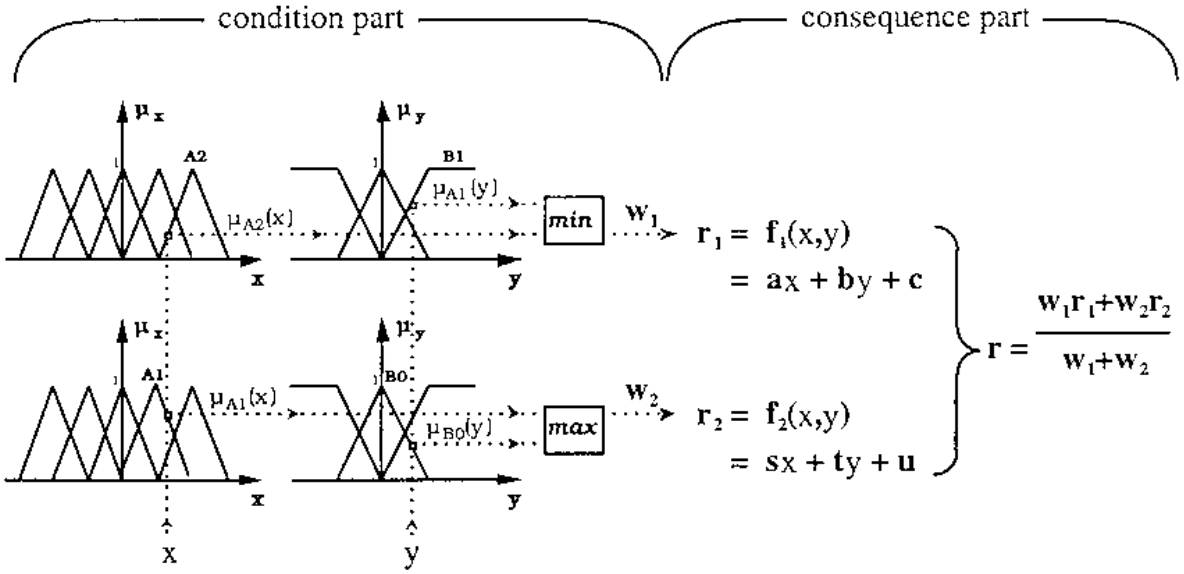

Figure 4. Takagi-Sugeno's method [13].

Jyh-Shing Roger Jang has presented the way by which it is possible to blend Artificial Neural Networks (ANN) and Fuzzy Implications systems. Fuzzy Implications are practical to make decisions based on a preset fuzzy rule set, but in itself it is a static implication that has been created by experiences. If the fuzzy parameters could be changed and optimized to the exact situation, the fuzzy inference would be more precise. To make a system adaptable, it must be capable of being taught, which creates the need for learning. With ANN it is possible to preset the parameters of the algorithm during a teaching phase. As Wang presented the Error Back-propagation minimize the distance among the desired target and the current output. The most effective solution is a gradient descent method where the gradient is the vector of the partial derivatives from the parameter's errors [15, 16].

As the authors have shown in Optimization of Big Population's Multimodal Biometrical Identification with a Complex neuro-Fuzzy Logic Controller, the ANFIS (Adaptive Neuro-Fuzzy Inference System) can combine the different biometric modals by qualitative indexes and makes it possible to learn some changes in the environment. The implemented ANFIS was trained by a Resilient Back Propagation, which was more suitable as an error back propagation method for learning. The outcome has shown that it is possible to find the correct number of epochs where the difference of the desired and the current output is minimal [17].

In the implemented algorithm two different inputs have been set, representing two biometric modalities in the ANFIS. The analogy is the following: each incoming dataset has to be compared to the other modalities by benchmark index, which is correlated to the quality of the dataset. For instance, the quality of a fingerprint sample has to be compared to the iris modal's quality. Following the comparison, the result of the ANFIS can determine the severity of the matching or the final decision which is made by the summing decision block.

RESULTS

With regard to the mathematical methods described above, a special combination of the statistical Bayes Theroem and a deterministic Soft Computing technique can describe an algorithm which is suitable and well-adapted to the typical failures of biometric identification. Figure 6 shows the mathematical framework of the implemented system.

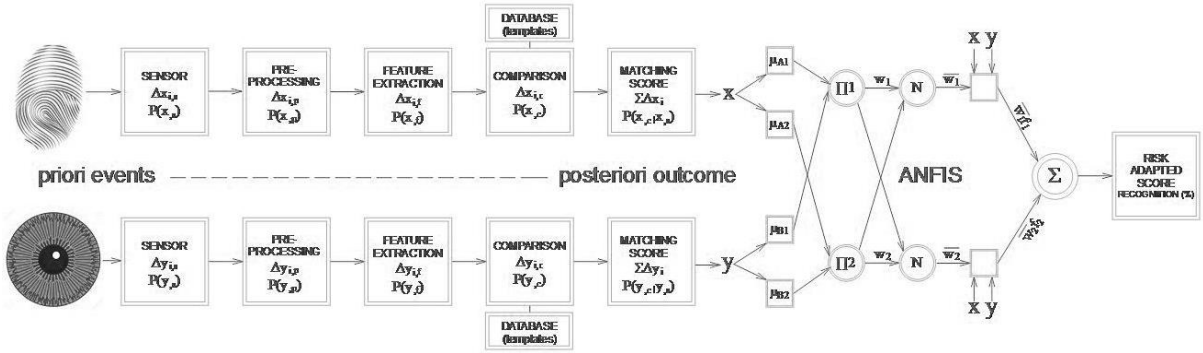

Figure 5. Algorithm of risk-adapted multimodal biometric identification.

The first part of the algorithm minimizes the effect of failure in the chain of the recognition process, while the second is a summation method that can be taught to detect the personal or local characteristics. The outcome is a risk adapted score, which is not a typical value, because it includes a correction unlike conventional biometrical outputs.

The method must be applied with caution, because there are preliminary steps that must be done properly, and tested before everyday use, just like in every solution that uses deep-learning.

CONCLUSIONS

The study has shown that the implementation of risk adaption in the authentication process is more than necessary, because the aggregated value of the risks can describe the suitable strength of the protocols. In some cases the boundaries of a biometric identification cannot be shifted with conventional methods, so it is worth using a multimodal process that can decrease the posteriori likelihood of systematic failures. The recognition can be even more accurate, if the scores of the matching passes through an ANFIS algorithm which has been taught in advance. Risk mitigation in the field of safety and security is a main objective, but usually there are only a few quantitative methods to decrease the invasive effect of natural impacts, such as environmental changes, human factor or frequent inadequate usage. With these modifications, the efficiency of access control systems can be increased, and the FRR and FAR can simultaneously improve. Therefore, the average time of access control can decrease even in highly secured installations.

REFERENCES

[1] Dolcourt, J.: *Vivo phone shows off first in-screen fingerprint scanner*. https://www.cnet.com/news/vivo-first-in-screen-fingerprint-scanner-for-phones-ces-2018, accessed 28th December 2018,

[2] NVIDIA Corporation: *Self-Driving Safety Report 2018*. https://www.nvidia.com/content/dam/en-zz/Solutions/self-driving-cars/safety-report/auto-print-safety-report-pdf-v16.5%20(1).pdf, accessed 28th December 2018,

[3] Haimes, Y.Y.: *In: Risk Modeling, Assessment, and Management*. John Wiley & Sons, Hoboken, Ch.2, 2005, http://dx.doi.org/10.1002/9780470422489.ch2,

[4] Jain, A.K.; Nandakumar, K and Nagar, K.: *Biometric Template Security.*
EURASIP Journal on Advances in Signal Processing **2008**, 1-17, 2008,
http://dx.doi.org/10.1155/2008/579416,

[5] Roberts, C.: *Biometric attack vectors and defences.*
Computer and Security, Department of Information Sciences **26**(1), 14-25, 2007,
http://dx.doi.org/10.1016/j.cose.2006.12.008,

[6] Ratha, N.K.; Connell, J.H. and Bolle, R.M.: *An Analysis of Minutiae Matching Strength*.
Proceedings of the 3rd International Conference on Audio and Video Based Biometric Person Authentication (AVBPA '01). Springer, Berlin, 2001,
http://dx.doi.org/10.1007/3-540-45344-X_32,

[7] Srivastava, H.: *A Comparison Based Study on Biometrics for Human Recognition.*
IOSR Journal of Computer Engineering **15**(1), 22-29, 2013,
http://dx.doi.org/10.9790/0661-1512229,

[8] Maurer, D.E. and Baker, J.P.: *Fusing multimodal biometrics with quality estimates via a Bayesian belief network*.
Journal Pattern Recognition **41**(3), 821-832, 2008,
http://dx.doi.org/10.1016/j.patcog.2007.08.008,

[9] Maurer, D.E.; Baker, J. P.: *Fusion of biometric data with quality esitmates via a Bayesian belief network*.
Proceedings of the Biometric Symposium, 2005,

[10] Rodrigues, R.N.; Ling, L.L. and Gondaraju, V.: *Roboustness of multimodal biometric fusion methods against spoof attacks*.
Journal of Visual Languages and Computing **20**(3), 169-179, 2009,
http://dx.doi.org/10.1016/j.jvlc.2009.01.010,

[11] Hanka, L. and Werner, G.: *Using the Beta-binomial Distribution for the Analysis of Biometric Identification*.
2015 IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY). IEEE, Subotica, 2015,
http://dx.doi.org/10.1109/SISY.2015.7325381,

[12] Zadeh, L.A.: *Fuzzy Sets*.
Information and Control **8**(3), 338-353, 1965,
http://dx.doi.org/10.1016/S0019-9958(65)90241-X,

[13] Sugeno, M. and Takagi, T.: *Derivation of Fuzzy Control Rules from Human Operator's Control Actions*.
IFAC Proceedings Volumes **16**(13), 55-60, 1983,
http://dx.doi.org/10.1016/S1474-6670(17)62005-6,

[14] Sugeno, M. and Takagi, T.: *Fuzzy Identification of Systems and Its Application to Modeling and Control*.
IEEE Transactions on Systems, Man, and Cybernetics **15**(1), 116-132, 1985,
http://dx.doi.org/10.1109/TSMC.1985.6313399,

[15] Jang, J-S.R.: *Fuzzy Modeling Using Generalized Neural Networks and Kalman Filter Algorithm*.
AAAI'91 Proceedings of the ninth National conference on Artificial intelligence **2**, pp.762-767, 1991,

[16] Wang, L.X. and Mendel, J.M.: *Back-propagation Fuzzy System as Nonlinear Dynamic System Identifiers.*
IEEE International Conference on Fuzzy Systems. IEEE, San Diego, 1992,
http://dx.doi.org/10.1109/FUZZY.1992.258711,

[17] Hanka, L. and Werner, G.: *Optimization of Big Population's Multimodal Biometrical Identification with a Complex neuro-Fuzzy Logic Controller.*
Sixth International Scientific Videoconference of Scientists and PhD students or candidates **31**(5), 2017.

Interdisciplinary Description of Complex Systems 18(3), 337-342, 2020

SECURITY ISSUES OF SMART CITY CONSTRUCTION

Richárd Pető*

Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering
Budapest, Hungary

DOI: 10.7906/indecs.18.3.2
Regular article

Received: 9 March 2020.
Accepted: 25 May 2020.

ABSTRACT

Building and operating a smart city must be based on a solid foundation. A stable foundation can only be built if all the necessary (security) elements are in place, and the connection among the elements is both established and functioning. It must be therefore clarified what security elements (areas of expertise) are required. The purpose of this article is to briefly present the security fields relating to smart city constructions and their interrelationships on the basis of the previous publication. By harmonizing the elements, risks can be reduced to an acceptable level.

KEY WORDS

IT, information, construction, construction yard, security, coordination, risk

CLASSIFICATION

JEL: D21, F52, G38, H11, H12, K00

*Corresponding author, η: Richárd Pető, petorichard.mk@gmail.com; +36 30 935 7667;
Hungary, 1096 Budapest Haller utca 20,

INTRODUCTION

In this article, the information technology (IT) approach to city/building constructions, and the construction of interconnecting systems have been discussed. Their significance is due to the fact that as early as the planning stage, a large amount of data (such as personal data, technical designs, financial documents, etc.) will be collected and managed, and they will be classified as confidential or even secret.

It should be taken into consideration that there are several buildings, objects, or things in which some type of a sensor is installed, and in some way they communicate the state of the systems or even the measured readings to the user. If this information is accessible to an unauthorized person, it can be misused, which will cause damage.

Two important facts can be deduced from the above information. The first is that nowadays it is increasingly difficult to mention anything that is not controlled by electronics or is not networked, which means that nearly everything communicates with the system user. The other fact is that as early as at the planning phase – that is well before any physical work is done on the construction site – significant risks can be expected [1].

EXAMINATION OF CONSTRUCTION PROJECTS

Sensitive information at risk (including later phases of the construction process) may include:

- (Day-to-day) organization plan (nature of workflows, workflow areas, company manpower, expected material deliveries, temporary and permanent storage areas, type and quantity of equipment and materials in warehouses and construction sites);
- construction plan of the structure of buildings;
- network and system blueprints for buildings (electrical network, water and sewage network, gas pipeline network, IT network, security system network, fire alarm network,);
- details of general contractor;
- regulations of the general contractor and those of the operation of the construction site;
- details of subcontracting companies;
- partnership contracts and commitments;
- performance confirmations and payments;
- official approvals;
- events and event logs;
- etc. [2, 3].

Data management may vary significantly from country to country. In the case of China, information gathering is centrally managed. Based on the data collected from different systems, the rights of the population are determined or even limited. When it comes to the European Union, it is the legal harmonization between the EU member states that plays an important role. Its objective is to develop and adopt regulations among the parties, which do not violate each other's rights. In recent years perhaps the best example of this effort has been "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", referred to briefly as the GDPR. Of the latter, it should be noted that it applies only to personal data, while it is not applicable to company secrets or confidential data [4].

Data and the networks that transfer them are omnipresent, and therefore, inevitable. The question is how these values can be protected. The answer is given through a complex system.

Basically, there are three main categories of data carriers [5, 6]:

- Persons as data carriers: A knowledge-based factor that may be intentionally or accidentally compromised.
- Hard copy (and traditional) media: This type includes various administrative tasks, treatment of documents and its entire process.
- IT-based media: The management of IT systems, including their operation, user management.

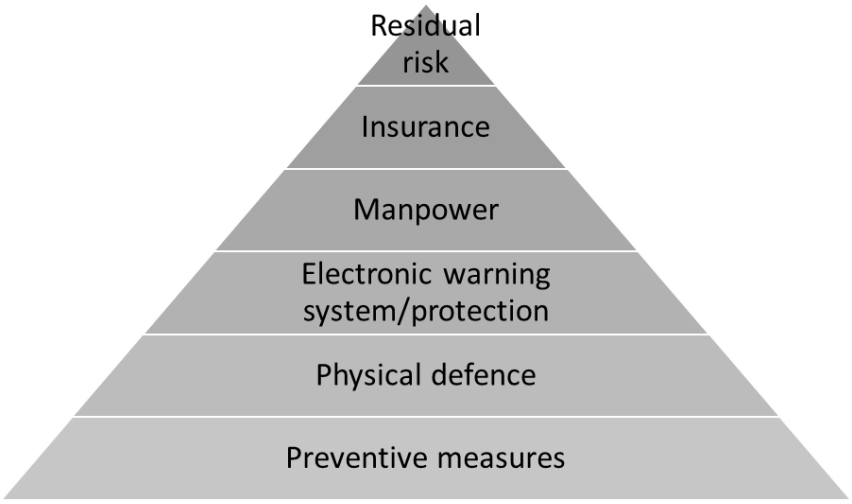

Figure 1. Steps of establishing security/safety (Security Pyramid)[1] [7].

The security pyramid provides a well-structured, general guidance. The security pyramid illustrates the components of protection and how they are built on one another. Each level has its own "mission" [8-12]. Each level can be further divided into sub-levels or components which may be called efficient, in dependence on having met the criteria. The summary of its levels (with reference to building protection):

The lowest level is made up by preventive measures. Basically, this is the fundament of the entire system, which is present anywhere at other levels as well. These measures include the introduction of and compliance with regulations and measures, without which other levels would be ineffective. For example:

- If the front door of a house is not closed, the physical protection built into the door, which is the lock in this case, will not serve its purpose.
- If the intrusion detection system is not armed, it will not signal the intruder.

The level of physical protection[2] consists of physical devices that make it difficult to enter or exit a given facility (e.g. a prison). Applying the previous example:

- If the door of a house is closed, but no built-in lock is available, no protection can be ensured in spite of any intention to protect the building.

The level of electronic signalling systems is responsible for signalling intrusions. The **fun**ction of various different sensors – movement, opening, breaking, vibration, sound etc. – is to signal in cases other than the "normal" (event-free) status. An electronic version of protection is an electronic device which is able to resist an intrusion regardless of its effect.

- The front door of a house has a lock and it is locked. If there is nothing to signal the alteration of normal status – e.g. in the case of a break-in, which is considered as a deviation from a "normal" status, that is the closed position –no protection will be provided.

The level of personnel is responsible for the immediate elimination of perceived adverse acts. This category includes the human force responsible for protection (bodyguards, security personnel, armed security guards, K-9 guards – the police in some respects – and trained (guard)dogs).

- The front door of a house has a lock and it is locked. If the intrusion detection system signals but there is no one to respond to the intrusion alarm, the necessary protection will not be achieved.

In spite of the security measures taken and established, a harmful event may occur in an unpredictable manner (for example, the attacker somehow gains access to the secured object, the fire extinguisher does not put out the fire, or not in the expected way, etc.), which may even be a chain of accidental events. In such cases it is the insurance service that will compensate the injured party.

The top level of the pyramid is represented by the so-called residual risk factors (also known as own risks). This level is always present, but its value or magnitude can be influenced. The more hazards are eliminated / minimized or the closer the probability of their occurrence is to zero, the lower its indicated value is. Since one cannot prepare for everything, this value can never equal zero.

There may also be a model similar to the security pyramid, which for simplicity will now be labelled as "extended security pyramid".

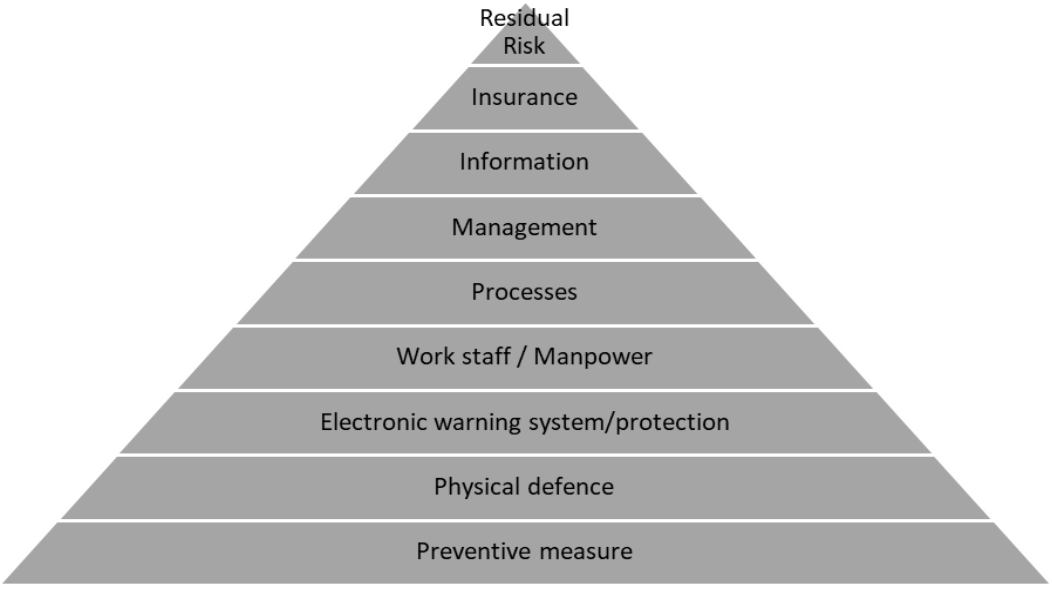

Figure 2. Steps of establishing security/safety (Extended Security Pyramid) [13].

The extended security pyramid has another three levels added:

- processes,
- management,
- information,

and at the level of labour force, the staff also appeares. A significant part of an organization is made up by employees who are not part of the security personnel. Through their involvement and security training, security risks can be reduced. Well-trained staff will initially be passive but later on, they get dynamically involved in security activities. Passive participation means simple compliance with the rules and regulations, while active involvement means noticing vulnerability or attack activities, and taking some action against them (signalling to security, recognising suspicious activities, etc.).

"Information" represents a significant part, as it comprises the basis of the decision-making process at management level. Various processes and their orders of execution are determined on the basis of information. These processes can be considered as the instructions of the organization. The composition of the instructions consists of the relevant legislation and the

internal, individual regulations of the organization. These regulations include, for example, the rules of the operation of the organization or organizational unit, the various organizational and production processes, or even the rights and obligations of guarding and security.

For those with no or limited security awareness the extended security pyramid gives a greater insight into how the system of the company works. In contrast, the other security pyramid consisting of fewer levels tends to be based on its main pillars, helping to make the levels more transparent and easier to memorise. Unlisted levels are included in various standards, and partly in legislation, each of which is integrated into different levels.

There are several examples to prove the above statements through asking and answering the following questions:

- Can a deal be concluded between a seller and a buyer if either of them is not aware of the other, or possibly of the product to be sold? Obviously not, because there is a lack of information and of its flow.
- The seller and the buyer can make a decision to sell or buy a product based on the necessary information. At this level (personal) management appears.
- What is the process of sale and purchase? The rules of the process (rules of procedure) are determined by the legislation and the participating parties. This is where the level of process appears.

The security pyramid (including the extended one) formulates levels that can be interpreted and applied as a system in other branches of security technology as well.
Returning to the original question of how values and valuables can be protected, the answer lies in the security pyramid shown above, that is, in the regulation and technology of its elements.

CONCLUSION

In the course of construction work, a large amount of data and information is transferred, most of which is classified as personal or confidential. If these data are not handled with due care, they can be compromised and easily misused. The article briefly summarizes what data could be involved and how it could be carried. Examining the above possibilities, it can be claimed that the key to the problem is the relationship between the security pyramids, the elements of the pyramid and their regulation.

REMARKS

[1]On the basis of other approaches, the structure of a pyramid or its levels would not be possible to interpret. E.g., 1) from an economic aspect, the budget of used solutions may significantly differ depending on the facility to protect, which means that the lowest level of the pyramid would not be made up by preventive measures. 2) in the interpretation of protective solutions, residual risk could not be interpreted. Through insurance, which is optional, it is only the extent of the harmful event that may be decreased, while the residual risk would not be involved in risk reduction. Nevertheless, this approach is applied here, because it can be interpreted as a general thumb rule, as a “technically” structured system.

[2]Mechanical protection may be a more precise term. the two terms are used here as synonyms.

REFERENCES

[1] Utassy, S.: *Komplex villamos rendszerek biztonságtechnikája*. Ph.D. Thesis.
Zrínyi Miklós Nemzetvédelmi Egyetem, Bólyai János Katonai Műszaki Kar Katonai Műszaki Doktori Iskola, Budapest, 2009,

[2] Buildingworld: *Organization plan.*
http://epitovilag.hu/organizacios-terv, accessed 17th June 2018,

[3] –: *No CXXXIII of 2005 Private security, and the activities of private investigators of the European Union.*
https://mkogy.jogtar.hu/jogszabaly?docid=a0500133.TV, accessed 4th February 2020,
[4] Horváth, Zs.: *Preface to IT security.*
In. *IT Security Engineer; Standard rules of IT security*.
Óbuda University, 2017,
[5] Constructible: *Cybersecurity In Construction: What You Need to Know*.
https://constructible.trimble.com/construction-industry/cybersecurity-in-construction-what-you-need-to-know, accessed 29th July 2019,
[6] MyIT: *3 Biggest Construction Cybersecurity Risks*.
https://www.myitsupport.com/3-biggest-construction-cybersecurity-risks, accessed 29th July 2019,
[7] The Chartered Institute of Building: *The role of security in the construction industry*.
https://www.ciob.org/sites/default/files/The_Role_of_Security_in_the_Construction_Industry.pdf, accessed 29th July 2019,
[8] –: *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, General Data Protection Regulation).*
https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=HU, accessed 11th November 2019,
[9] Berek, L.; Berek, T. and Berek, L.: *Security*.
Óbudai University Donát Bánki faculty of mechanical and safety engineering, Budapest, 2016,
[10] Horváth, Zs.: *Az információbiztonsági irányítási rendszer alapjai.*
https://anzdoc.com/az-informaciobiztonsagi-iranyitasi-rendszer-alapjai.html, accessed 14th December, 2018,
[11] Berek, L.: *Biztonságtechnika, Nemzeti Közszolgálati Egyetem.* In Hungarian.
http://real.mtak.hu/19709/1/biztonsagtechnika.original.pdf, accessed 8th September, 2018,
[12] Pető, R.: *Safety and Security of Constrution sites.*
Óbuda University, Budapest, 2019,
[13] Papp, R.: *Pyramid of Security.*
Óbudai University Donát Bánki faculty of mechanical and safety engineering, Budapest, 2016.

Interdisciplinary Description of Complex Systems 18(3), 343-351, 2020

AUTOMATED VEHICLES RISK ASSESSMENT AND EVALUATION

Malak M. Shatnawi*

Óbuda University, Doctoral School on Safety and Security Science
Budapest, Hungary

DOI: 10.7906/indecs.18.3.3
Regular article

Received: 28 April 2019.
Accepted: 25 May 2020.

ABSTRACT

Statistics show that the number of passenger cars is increasing significantly, which will have a negative impact on social, economic and environmental sustainability, and it will cause severe problems for the next generations. Automated Vehicles represent an innovation in automotive technology. They have become a global concern because of their importance in smart traffic systems as well as their significant impact on safety, supposing that traffic will be more efficient and longer travel distance will not be a problem. They will become more acceptable since they will encourage living in suburbs and leaving noisy and polluted cities behind. Drivers will be more relaxed and in comfort while enjoying travel time and some extra privileges that they may have, for example, the chance for spending time more productively and efficiently at non-driving times inside the vehicle. Automated Vehicles are also beneficial for the environment. In fact, it is expected that in the next few years these cars in general will provide a solution for many problems. Researchers and planners of transportation systems are facing many challenges in the field of autonomous vehicles, as the level of safety and mobility involves such elements and circumstances which may cause that the operated travel will be less efficient than expected. The aim of the article is to discuss the challenges, threats, vulnerability, impacts and likelihood of failure faced in the development of Automated Vehicles by studying information security risk management standard process, and explaining how to apply the process of International Organization for Standardization. The concept of applying ISO to Automated Vehicles will be discussed here through certain processes.

KEY WORDS

autonomous vehicles, risk management, risk assessment, transportation, safety and security

CLASSIFICATION

JEL: O10, Q55

*Corresponding author, η: malak.shatnawi@phd.uni-obuda.hu; +36 20 514 3327;
Népszínház street 8, Budapest, 1081, Hungary

INTRODUCTION

Autonomous vehicles (AVs) are vehicles which are capable of driving themselves as well as recognizing, handling and sensing their environment. In order to do this, these vehicles should make decisions about where it is safe and desirable to move without the need for human supervision, control or operation. Everyone in the car could be a passenger, or it could even drive with no occupants at all. Automated vehicles are becoming a global phenomenon and expected to have various social, economic and environmental benefits. In fact, they are designed so that in the future they will be the solution for transportation systems, because of their high priority in achieving safety, not to mention other potential benefits. In the domain of Automated Vehicles there have been many different studies recently. Transport researchers generally focus on the implementation of intelligent transport systems (ITS), for example, how to construct and develop roads and traffic for a transport automation system with partially or fully autonomous vehicles, which will have a strong impact on the automotive industry and on the whole transportation system. Moreover, in the near future, self-driving cars will fundamentally reformulate road transportation inducing technological and socio-economic developments and requiring adaptation of the applicable laws as well as social acceptance. The framework is continuously changing over time, i.e. the future transportation design has to take into consideration technical, economic, legal, and social aspects simultaneously [1]. Software in AVs has various roles: engine control, external communications, car safety and security, and from the point of security the primary aim is to build a cyber-safe system with regard to the vehicles, vehicle systems and the intelligent infrastructure within the intelligent transport system [2]. The implementation of AVs will produce safer roads by removing human error from the driving equation, cleaner, healthier environment, new culture of sharing rides, which could reduce the need for new roads or parking areas and the expansion of existing roads, creating the potential to construct space for uses such as businesses, green space, walking and bicycling infrastructure. In addition, AVs will significantly improve traffic behaviour, as drivers will be more relaxed and enjoying travel time. Some expected benefits of exploiting non-driving time in vehicles in a productive way, transport accessibility to be widened for those previously unable to drive and it will improve access to certain jobs.

With a shift towards autonomous technology and away from human operators, vehicles are autonomously restored to the system state of minimal risk. From a technical point of view, the greatest challenge lies in the complete absence of a human supervisor, who knows the system's limits, recognizes its faults and, where needed, switches the vehicle into a safe state. But first, the meaning of a safe state must be defined, and whether it is possible for a driver take control within the exact needed time. Especially on highways these questions need to be further tested, analysed and assessed to identify the impact [3]. Special attention must be paid to the discussion of safety challenges that a self-driving electrical car project can encounter, and the main outcomes and future research possibilities for development [4]. Also, motor insurance companies, and related parties may change dramatically. There would be a greater need for the expertise of data analysts to understand why an autonomously operated vehicle failed in the event of an accident, and other potential negative impacts cannot be neglected. For example, who will take liability and blame for accidents, what happens to those millions who will be out of work, especially unskilled people. Therefore, the consequences of the use of this technology must be further studied. On the other hand, strategies must ensure that all adapted policies must be for the benefit of the whole community to create a better future for transportation, rather than focus narrowly on serving only vehicles. From an environmental point of view, it is known that Europe's primary sources for obtaining electricity rely heavily on coal, oil, gas and nuclear energy, and the goal should be to look for new energy sources (renewable and /or non-fossil sources) and to invest in better management and technologies

to reduce pollution. Since the energy consumption of the transportation sector is continuously increasing, more efficient and modern strategies are required in order to reduce its negative impact. It will have direct and indirect impact on transportation infrastructure and its environmental dimensions of sustainability for the coming generations. Whether the outcomes are positive or negative, it will depend on how policy frameworks guide the introduction of this rapidly evolving technology. The structure of the article is the following: the first part contains the literature review, it addresses the sustainability of using AVs with emphasize on positive and negative sustainability dimensions, impacts, risk management and assessment. The second part of this article describes the methodology of the research and introduces the concept of AV with risk management and risk assessment according to International Standardization. The final part includes the conclusions and recommendations.

LITERATURE REVIEW

New technology always come with new risks, and the fear of autonomous vehicles is quite significant. However, increased safety, efficiency and improvements in quality of life and work are worth the effort, for instance globally, 93 % of road traffic accidents are caused by human error, with 1,3 million fatalities and 50 million injuries every year. By replacing the fallible human driver with a sufficiently capable technology, it is thought that collision rates will substantially decrease, with significant implications on safety. The potential for change is great, and yet, at the same time, this must be balanced against the practicalities of implementation, and the achievement of adequate safety standards to mitigate the new risks that come with the new technology. The lengthy considerations that would have to lead to reworking laws, systems and infrastructure should not be underestimated, nor should public mistrust of putting lives in the hands of technology.

TRANSPORTATION SUSTAINABILITY

Sustainability in general is gaining balance between three main pillars: the economic, environmental and social health of a community. However, sustainability from transportation perspective, as reviewed in most literatures, is the future capacity to enhance mobility needs of a society to be less harmful for the environment with respect to the mobility needs for the generations to come. The European Council of Ministers of Transport (ECMT) defines a sustainable transportation system as one that meets the following: -

1. Allows the basic access needs of individuals and societies to meet safely and in a manner consistent with human and ecosystem health, and with equity within and between generations.
2. Affordable, operates efficiently, offers choice of transport modes, and supports a vibrant economy.
3. Limits emissions and waste within the planet’s ability to absorb them, minimizes consumption of non-renewable resources, limits consumption of renewable resources to the sustainable yield level, re-uses and re-cycles its components, and minimizes the use of land and the production of noise.

AVS AND SUSTAINABILITY DIMENSIONS

By applying the definitions of a sustainable transportation system on AVs according to (ECMT) most of the elements to reach sustainability have been achieved.

THE SOCIAL DIMENSION

Many advantages have been associated with AVs recently. Handicapped or disabled people consider such cars as blessings. It will bring the chance for minors to move on road without adults joining them. They will enrich the travel experience and bring excitement and release people who do not like driving from this burden, as the car’s intelligent system will choose

the most optimal route decreasing highway traffic jams. All of these and more needed to be analysed to inform decision makers and to support risk responses [5]. Studies show that more than 90 % of automobile related fatalities are attributable to human error, either negligence, distraction, incapacitation or other human factors. Therefore, safer transportation with no human error is the most significant benefit, since the ability to control the flow of traffic will greatly increase. It is also worth to mention that a major strength of automated driving is that stress would no longer be a part of daily life and the morning commute to work would be relaxing.

THE ECONOMIC DIMENSION

There will be indirect impacts on the economy, because autonomous cars will cause cities to expand and they will reduce parking lots, which will make valuable land available for development and allow cities to grow. Furthermore, longer travel distance will not be a problem, on the contrary, it will be more acceptable and it will encourage living in suburbs and leaving noisy and polluted cities behind, which will increase prosperity of such areas for the benefit of the economic dimension of both cities and suburbs.

THE ENVIRONMENTAL DIMENSION

The preparation to shift towards another system of transportation could also become the perfect opportunity to incorporate more electric technology into automobiles, thus reducing carbon-emissions. From an optimistic point of view, the positive result is that using renewable energy sources for electricity generation will result in an over 25 percent reduction in emissions. It is shown by statistics that emissions of electric vehicles are falling. With declining percentage of electricity generated by coal power and increasing renewable resources, as well as with continued improvements in vehicle technologies the emissions reduction benefits of EVs will continue to grow. By 2050, much greater deployment of renewable energy sources could lower global warming emissions even further. Studies include electricity produced from renewable sources, under which scenario, emission intensity will be reduced. Also, driving at more consistent speeds, with less accelerating and braking, as well as more efficiently chosen routes could result in lower carbon emissions from driving. On the other hand, the initial concern and fear should be replaced by complete reliance on technology, and since driving can be a very dangerous task, it should be let under the control of an automated system. The infrastructure should also be made ideal for such fully automated vehicles, and it will take long to develop such an ideal infrastructure. A massive amount of data needs to be collected and tested via field before implementation. Other questions will come to surface related to various situations, for example, the liability of accidents, whether is it the responsibility of the car owner or the manufacturer, how the insurance company will deal with it, whether for the priority of safety the vehicle will take the right decision, and there will be an enough time for the driver to interfere, as well as many other questions. Also if we want the system to operate efficiently, there must be a single, ultimate network on which these vehicles communicate and operate with one another, since the cars are essentially computers on wheels, they do face cybersecurity threats. Many concerns about privacy and personal information security will arise not to mention the passengers' location which can be tracked. All of these are considered as weakness points and threats, and, at the same time, many parties will be affected either directly or indirectly, for example, but not limited to, auto manufacturers, oil companies, labour sectors, job seekers, etc.

METHODOLOGY

As the process of research in automated transportation is a combine of an unlimited set of operational scenarios encountered in public traffic with the absence of human supervision, it needs the

highest demands regarding functional safety throughout the development of these systems. To ensure safety, a risk assessment must be carried out, with analysis and evaluation as well.

RISK MANAGEMENT AND ASSESSMENT PROCESSES

It is a fact that in recent research special attention has been paid to the discussion of the safety challenges that a self-driving electrical car project can encounter, the main outcomes and future research and development possibilities [4]. Hence, risk management is brought to surface in this research as it aims to make the transportation system more secure in terms of traffic accidents, protection against theft, security of software systems against malfunctions and external attacks. Software in AVs has various roles: engine control, external communications, car safety and security, and to build a cyber-safe system with regard to the vehicles, vehicle systems and intelligent infrastructure within the intelligent transport system [2].The main challenges in the field of autonomous vehicles rest in the fact that it will result in "Improving road safety by removing human error from the driving equation, through testing and validation processes for new autonomous systems and features and through developing cost and time efficient methodologies" [6]. There are continuous changes in the fields of research over time, i.e. future transportation design has to take into consideration technical and economic aspects as well as, legal rules and regulations, financial, insurance policies, socio-economic benefits, and other necessary factors [1]. The concept of applying NIST SP 800-30 and International Organization for Standardization (ISO)/ International Electro Technical Commission (IEC) 27005 to AV will also be discussed [5]. By implementing the risk assessment process, threats and vulnerabilities and their impact will be studied, and the analysis of risks will be followed by evaluation, whether they should be accepted or treated, and each step will be compatible and correlative with monitoring, acceptance, communication and consultation steps, as it is show in Table 1 and 2 below.

RISK ASSESSMENT

Risk assessment does not only depend on ideal design system and modern technology implementation but also on seeking for information and data from different realistic studies. With the help of all possible assistance from transportation researchers and planners, the risk assessment process must be identified, analysed and evaluated, and each step in the assessment process must be implemented. This article supports the general concepts specified and designed as guidelines for security risk management and to define the approach to the risk management process as seen in the Tables below [5]. The assessment processes for risks will be as follows.

Risk Identifications

Self-driving vehicles are not yet completely present in the traffic streams, with the exception of a few test vehicles. It is difficult to reliably predict future consumer demand. Any outcomes are just theoretical at this point since the fully self-driving technology is not available on the streets, the expectations of using self-driving cars are still not clear depending on how and when people will use self-driving vehicles [7]. This is why different risk studies are associated with the self-driving vehicles technology and each must be carefully assessed and taken into account [4].

Risk Analysis

If any interruption occurs to an AV’s system, this will lead to high economic, environmental and social damages and leave the whole system in huge danger [8].

Table 1. Risk analysis.

Resource and Assets	Automated vehicles are not yet involved in the traffic and passenger demands are still ambiguous and uncertain, whether it will increase or decrease. To solve such problems and to make people more trusted in such technology, the following must be tested, assessed and evaluated; infrastructure readiness with existing as well as modern technology, and smart systems, in addition to the information and data implementation.
Threats	It is a very important to analyse in order to predict the needed processes to apply to the whole automated system, and to identify the types of threats that will surface first, the threats on infrastructure itself should be examined, because at present, there is no separated automation infrastructure, so automated vehicles should be made alert to their surroundings, other objects, cars, infrastructure and electric system, and their security aspects against direct or indirect contacts. At the same time, the operational and functional system safety in the car itself is a very important and vital element, since it is mainly concerned about hardware failures and software bugs [4]. To solve such problems and to analyse such threats the impact of cyber security must be taken into consideration, because these vehicles will be increasingly connected with smartphones and tablets. Even now, cars already have computerised units, so it is better to be worked by isolated systems, not networked, and therefore at less risk and less hacker attacks to access personal data.
Vulnerability and Impact	Analysis of the expected vulnerability and impacts include: - 1. Direct and indirect interruption or deliberate corruption occurred and how it will lead to severe economic, social and environmental damages and leave the whole system at risk 2. Battery charging safety and vehicle maintenance, 3. Operation and training and 4. With the identification of priority areas according to risk degree, in order to rearrange risks to an acceptable risk degree [4].
Likelihood of Failure	"Every type of sensor has weaknesses, for example the weather condition has a strong effect on the visual capability of the video-based sensors. From another aspect, disturbances can also be simulated by region dependent road types or traffic signs" [6].

Risk Evaluations

By using certain electronic systems and sensors to observe the environment and for mapping, localisation and navigation, such as a Vehicle-to-Everything platform, a vehicular communication system that incorporates other more specific types of communication as (Vehicle-to-Infrastructure), (Vehicle-to-Vehicle), (Vehicle-to-Pedestrian) or other users such as cyclists or a Wi-Fi network by providing automatic warning to prevent an accident, (Vehicle-to-Device), (Vehicle-to-Grid), or any other entity that may affect the vehicle [4].

The behaviour of pedestrians or a person around the car is difficult to predict in order to react properly. "In case of a sudden reaction of a person, the system must be able to react and remain in a safe state. This holds also for people lying on the ground or small animals. After all, these are not imaginary but fully realistic situations; in case a collision occurs, the system has to be able to stop so that no injury occurs" [4].

Table 2. Monitoring, acceptance, communication and consultation.

Monitoring Risk and Risk Treatment	This can be achieved by testing the self-driving functions of the vehicles within a controlled area as a "Smart City". A "Smart City" would be "a place where connected car features and smart traffic control systems could monitor and test the conventional traffic stakeholders, as well as the automated vehicles using the controlled, partially public road. The modified regulation of the traffic could be time dependent and it would be dynamically changeable to meet the safety objectives at all times" [6].
Risk Acceptance	Risk can be at an acceptable rate if the followings are maintained: - 1. Comfort, safety, velocity and traffic density, 2. Increased productivity (transport capacity), 3. Decreased or even eliminated traffic jams with efficient and intelligent traffic control systems, 4. Reduced number of accidents and 5. Reduced emission of harmful materials, where the smart city transport can be conceived as an advanced ITS system [2].
Risk Communication and Consultation	If self-driving cars could approach people whenever and wherever needed, it would lead to less car parks and less ownership of private cars. Safety and productivity are also added to socio-economic benefits, including sharing. This, however, will require public acceptance and usage before experiencing the benefits, and users will create the demand that will determine the size of market development. "The advent of autonomous vehicles could be truly transformative" [7]. Academic and non-academic sources have discussed the numerous advantages of AVs and how they will reduce the cost of travel, allow minors to travel without the presence of adults, enhance travel experience, travel more safely, or choose the route more optimally. But the questions arise, how other transportation modes, such as travel by Traditional Vehicles (TVs) or no travel at all, will be affected by such innovation, what effects it will have on the labour force, how the role of motor insurance companies can be determined, as losses may not be associated with one particular party, etc. [9]. In addition, in case of an accident, it must be determined who will take the risk and accept liability: the manufacturing company, the software provider or others, and how these vehicles could be protected from hackers and severe attackers [10].
Risk Monitoring and Review	Automated Vehicles AV will be able to move with the help of an intelligent driving system that will replace human driving, and this will raise a number of issues. For example, initiative studies must be made for empty AVs from central to external parking in the morning, and vice versa in the evening, as traffic is expected to increase with the introduction of AVs, but this will not necessarily cause congestion. In fact, it will reduce traffic accidents and increase safety. "Create smoother traffic flow and unlock existing capacity on roadways which means less road works" [7].

CONCLUSIONS AND RECOMMENDATIONS

When an Information Security Management System (ISMS) is applied to Automated Vehicles AV with risk management in a systematic way, the following social, economic and environmental dimensions will be achieved to maintain welfare for the whole society. It will change the lifestyle of driving and passengers, as it will change many people's habits by

making life easier, saving time and removing many obstacles and burdens, as it promotes travelling for long distances, allows minors to travel without the presence of adults. It will relieve busy people, elderly and people who are afraid of driving from the burden of driving,

Reduced costs of parking and other costs as compared to travelling by traditional vehicles will make people accept longer travel distances in exchange for larger and more comfortable family residences, which will increase the total size of residential land that was previously considered to be too far away.

People will travel more safely, choose the route more optimally, increase highway usage and this will enrich travel experience.

In addition, cities will change, urban and rural planning will proceed in a different direction to be compatible with the latest developments in the traffic and transportation technology using appropriate infrastructure. Less parking space will be needed especially in downtowns, as daytime parking will become unnecessary, which allows the use of urban land that was dedicated to parking.

The size and density of economic activity will grow, causing increase in productivity.

Although traffic is expected to increase, this will not necessarily cause more congestion, as AVs are expected to operate more efficiently.

For further research in the future it is recommended to adopt creative and initiative studies for empty AVs in the morning because the reverse traffic will be made by mostly empty AVs and vice versa in the evening.

As long as Traditional Vehicles and Automated Vehicles travel together the risk will be higher, which means that governments should adopt more traffic control systems and encourage car sharing for AVs in all possible ways, especially in rush hour periods.

Threats related to cyber security must be considered for further innovative studies, and it is better to work in isolated safe systems, not networked, so that hacker attacks cannot access personal data or take control of the AV system.

ACKNOWLEDGEMENTS

I would like to acknowledge my supervisor as well as my family for their support. Also I would like to acknowledge the reviewers and the organizers of SSSCC 2019 Conference and Obuda University.

REFERENCES

[1] Tettamanti,T.; Varga, I. and Szalay, Zs.: *Impacts of Autonomous Cars from a Traffic Engineering Perspective*.
Periodica Polytechnica Transportation Engineering **44**(4), 244-250, 2016,

[2] Tokody, D.; Albini, A.; Ady, L.; Rajnai, Z. and Pongrácz, F.: *Safety and Security through the Design of Autonomous Intelligent Vehicle Systems and Intelligent Infrastructure in the Smart City.*
Interdisciplinary Description of Complex Systems **16**(3-A), 384-396, 2018,
http://dx.doi.org/10.7906/indecs.16.3.11,

[3] Maurer, M.; Gerdes, C.J.; Lenz, B. and Winner, H.: *Autonomous Driving, Technical, Legal and Social Aspects.*
Springer-Verlag GmbH, Berlin, 2015,

[4] Rassõlkin, A.; Sell, R.; Leier, M.: *Development Case Study of the First Estonian Self-Driving Car.*
Electrical, Control and Communication Engineering **14**(1), 81-88, 2018,
http://dx.doi.org/10.2478/ecce-2018-0009,

[5] ISO Standard: *ISO/IEC 27005:2018, Information technology – Security techniques – Information security risk management*

[6] Szalay, Zs.; Nyerges, A.; Hamar, Z. and Hesz, M.: Technical Specification Methodology for an Automotive Proving Ground Dedicated to Connected and Automated Vehicles. Periodica Polytechnica Transportation Engineering **45**(3), 168-174, 2017, http://dx.doi.org/10.3311/PPtr.10708,

[7] Zmud, J.P and Sener, I.N.: *Towards an Understanding of the Travel Behavior Impact of Autonomous Vehicles.* Transportation Research Procedia **25**, 2500-2519, 2017, http://dx.doi.org/10.1016/j.trpro.2017.05.281,

[8] Pleskonjic, D.; Virtuani, F. and Zoggia, O.: *Security Risk Management for Critical Infrastructures.* https://www.researchgate.net/publication/267924586_Security_Risk_Management_for_Critical_Infrastructures, accessed 16th April 2019,

[9] Zakharenko, R.: *Self-driving cars will change cities.* Regional Science and Urban Economics **61**, 26-37, 2016, http://dx.doi.org/10.1016/j.regsciurbeco.2016.09.003,

[10] Hazel, S.M.L. and Taeihagh, A.: *Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications*. Energies **11**(5), 1-23, 2018, http://dx.doi.org/10.3390/en11051062.

Interdisciplinary Description of Complex Systems 18(3), 352-359, 2020

INTUITIONISTIC FUZZY RULE-BASE MODEL FOR THE TIME DEPENDENT TRAVELING SALESMAN PROBLEM

Ruba S. Almahasneh[1] and László T. Kóczy[1, 2, *]

[1]Budapest University of Technology and Economics
Budapest, Hungary

[2]Széchenyi István University
Győr, Hungary

DOI: 10.7906/indecs.18.3.4
Regular article

Received: 6 September 2019.
Accepted: 1 June 2020.

ABSTRACT

The Traveling Salesman Problem is a well-known combinatorial optimization problem. There are many different extensions and modifications of the original problem, such as The Time Dependent Traveling Salesman Problem, this specific extension of the original Traveling Salesman Problem towards more realistic traffic conditions assessment. In the Time Dependent Traveling Salesman Problem the "distances" (costs) between nodes vary in time, they are considered longer during the rush hour period or in the traffic jam region, e.g. the city centre. In this article we introduce an even more realistic approach, the Intuitionistic Fuzzy Time Dependent Traveling Salesman Problem. It is an extension of the Time Dependent Traveling Salesman Problem with the additional notion of intuitionistic fuzzy sets (which is a generalization of the original fuzzy sets). Our goal is to give a useful extended, alternative model instead of the original abstract problem. By demonstrating that the addition of intuitionistic fuzzy elements to quantify the intangible jam factors creates an inference system that approximates the tour cost in a more practical way. Hence, we are one step closer to offering a more realistic solution for the generalized Traveling Salesman Problem. The results of two simple toy examples showed the general effectiveness of the model.

KEY WORDS

intuitionistic fuzzy sets, time dependent traveling salesman problem, traveling salesman problem, intuitionistic fuzzy time dependent traveling salesman problem

CLASSIFICATION

JEL: C44

PACS: 07.05.Mh

*Corresponding author, η: koczy@sze.hu; +36 30 552 3070;
1117 Budapest, Magyar tudósok körútja 2. I.B.224

INTRODUCTION

The Traveling Salesman Problem (TSP) is one of the most extensively studied NP-hard graph search problems [1]. In the literature, there have been numerous published approaches for quality solutions, applying various techniques in order to find the optimum (least cost) or semi optimum solution. There are many different extensions and modifications of the original problem, such as The Time Dependent Traveling Salesman Problem (TDTSP) [2], this specific extension of the original TSP towards more realistic traffic conditions assessment. In the literature many researchers applied different methods in attempt of solving the TDTSP [3]. Here we propose a novel approach using fuzzy numbers, since we look at the jam regions and rush hours as uncertain factors that cannot realistically be represented with crisp numbers. In 1965, fuzzy sets as an extension of classical notion of set were introduced by L.A. Zadeh [4]. According to that, membership functions ranging in the unit interval [0, 1] can help to describe such phenomena as uncertain extension of the jam region (an uncertain sub-graph of the original complete graph), and the uncertain timely extension of the rush hour period, more efficiently. On the other hand, there are several generalizations of fuzzy set theory for various objectives; the notion of intuitionistic fuzzy sets (IFSs) introduced by Atanassov [5] is an interesting and useful one. Fuzzy sets are (special) IFSs but the converse is not accurately true [6]. In fact, there are situations where IFS theory is more convenient to deal with [7]; the TDTSP with jam factors is a prime example. In addition, it has been shown by several researchers that realistic sets with uncertainty factors may be properly modelled by IFSs. IFS theory has been applied in different areas that have to do with decision making under high hesitation and vagueness degrees and it prove being successful. In the present article we study the extended TDTSP problem using the notions of IFS theory by introducing the broadened model.

THE INTUITIONISTIC FUZZY TIME DEPENDENT TRAVELING SALESMAN PROBLEM (IFTD TSP)

In the TDTSP the goals is to calculate the time required to cover the distance between cities is vital. Since the cost elements are time dependent, then the actual cost between two cities can be determined only if the total time elapsed is precisely resolved. Considering an actual salesman tours, especially in city centres, the topography and rush hours in variant locations are factors that must be looked at as uncertain or vague values, more precisely as fuzzy numbers. Hence, relevant data for estimated tour distance between two nodes is not constant as suggested previously In the classic TDTSP [2]. On the contrary, it can be more appropriate to represent this imprecision using the intuitionistic fuzzy model. This in turn will introduce more realistic trips measurements and ultimately optimized solution for TDTSP problem with traffic jam factors. In the following section we will go through some definitions before we apply our propsed model on a sample tour and prove its efficiency.

DEFINITIONS

Let us start with a short review of basic concepts and definitions related to intuitionistic fuzzy sets which are used in the upcoming sections.

DEFINITION 1

Let a universal set E be fixed. An intuitionistic fuzzy set or IFS A in E is an object having the form

$$A = \{\langle x, \mu_A(x), v_A(x) \rangle | x \epsilon E\}, \tag{1}$$

where $0 \leq \mu_A(x) + v_A(x) \leq 1$. The amount $\pi_A(x) = 1 - (\mu_A(x) + v_A(x))$ is called the hesitation part, which may cater to either the membership value or to the non-membership value, or to both.

DEFINITION 2

Let E be a nonempty classical set and let A and B be intuitionistic fuzzy sets of E, then

$$A \subset B \text{ if and only if}$$

$$\forall\, x \in E, \begin{bmatrix} \mu_A(x) \leq \mu_B(x) \text{ and} \\ v_A(x) \geq v_B(x) \end{bmatrix}. \tag{2}$$

$$A \supset B \text{ if and only if } B \subset A$$

$$A = B \text{ if } \forall x \in E, \begin{bmatrix} \mu_A(x) = \mu_B(x) \text{ and} \\ v_A(x) = V_B(x) \end{bmatrix}. \tag{3}$$

$$A \cap B = \{\langle x, min(\mu_A(x), \mu_B(x)), max(v_A(x), v_B(x))\rangle | x \in E\}, \tag{4}$$

$$A \cup B = \{\langle x, max(\mu_A(x), \mu_B(x)), min(v(x), v_B(x))\rangle | x \in E\}, \tag{5}$$

$$\{\langle x, \mu_A(x), \mu_{A^c}(x)\rangle | x \in E\},$$

where A^c is the complement of A.

DEFINITION 3

Let X and Y be two nonempty classical sets. An intuitionistic fuzzy relation (IFR) R from X to Y is an IFS of X × Y, characterized by the membership function μ_R and the non-membership function v_R. An IFR R from X to Y will be denoted by R(X→Y).

DEFINITION 4

If A is an IFS of X, the max-min-max composition of the IFR R (X → Y)with A is an IFS B of Y denoted by (B = R∘A); and is defined by the membership function

$$\mu_{R\circ A}(y) = \vee_x[\mu_A(x) \wedge \mu_R(x, y)], \tag{6}$$

and the non-membership function

$$v_{R\circ A}(y) = \wedge_x[v_A(x) \vee v_R(x, y)], \tag{7}$$

$$\forall y \in Y\ (\wedge = Min\ and\ \vee = Max).$$

DEFINITION 4

Let Q(X → Y) and R(Y → Z) be two IFRs. The max-min-max composition (R ∘ Q); is the intuitionistic fuzzy relation from X to Z, defined by the membership function

$$\mu_{R\circ Q}(x, z) = \vee_y[\mu_Q(x, y) \wedge \mu_R(y, z)], \tag{8}$$

and the non-membership function given by

$$V_{R\circ Q}(x, z) = \wedge_y[v_Q(x, y) \vee v_R(y, z)], \tag{9}$$

$$\forall (x, z) \in X \times Z\ and\ \forall y \in Y).$$

IFTDTSP

In the TSP, the salesman originally attempts to find the optimal (shortest) route starting from the initial node (company headquarters), so that all nodes (cities, shops or other locations on

the agenda) are visited exactly once and then returns to the starting point [1]. We suppose E is a set of edges; where the edge is the distance between two nodes as shown in (Figure 1). Each edge possesses a fuzzy jam factor due to the topography of the paths between cities (nodes). C is the set of jam factor costs (for short we will refer for it from now on as costs). We define an intuitionistic fuzzy relation R from the set of jam factor J to the set of C (i.e., on J × C) which reveals the degrees of association and of non-association between jam factor and cost.

There are three main steps that formulates the core of our IFTSTSP model:

1. Determination of edges that have jam factors.
2. Formulation of cost knowledge based on intuitionistic fuzzy relations.
3. Determination of cost on the basis of composition of intuitionistic fuzzy relations.

Let A be an IFS of the set J, and R be an IFR from J to C. Then the Max-Min-Max composition as in Equations (8) and (9), B of IFS A with the IFR R(J → C) denoted by B = A ∘ R signifies the cost of the edges as an IFS B of C with the membership function given by

$$\mu_B(c) = \vee_{j\epsilon J}[\mu_A(j) \wedge \mu_R(j,c)], \tag{10}$$

and the non-membership function given by

$$v_B(c) = \wedge_{j\epsilon J}[v_A(j) \vee v_R(j,c)], \tag{11}$$

$$\forall c \in C. (Here\ \wedge = Min\ and \vee Max).$$

If the state of the edge *E* is described in terms of an IFS *A of J*; then *E* is assumed to be the assigned cost in terms of IFS *B of C*, through an IFR *R* from *J* to *C*, which is assumed to be given by knowledge base directory (or experts who are able to translate the jam degrees of association and non-association according to geographical areas) on the destination cities and the extent (membership) to which each one is included in the jam region. This will be translated to the degrees of association and non-association, respectively, between jam and cost. Now let us expand this concept to a finite number of edges *E* that form a whole tour for a salesman. Let there be *n* edges E_i; $i = 1, 2, ..., n$; in a trip (from starting point to final destination). Thus $e_i \in E$. Let *R* be an IFR (J → C) and construct an IFR *Q* from the set of edges *E* to the set of jam factors *J*. Clearly, the composition *T* of IFRs *R* and *Q* $(T = R \circ Q)$ give the cost for each edge from *E* to *C* given by the membership function

$$\mu_T(e_i, c) = \vee_{j\epsilon J}\left[\mu_Q(e_i, j) \wedge \mu_R(j,c)\right], \tag{12}$$

and the non-membership function given by

$$v_T(e_i, c) = \wedge_{j\epsilon J}\left[v_Q(e_i, j) \vee v_R(j,c)\right]. \tag{13}$$

$$\forall e_i \in E\ and\ c \in C.$$

For given *R* and *Q*, the relation $(T = R \circ Q)$ can be computed. From the knowledge of *Q* and *T*, an improved version of the IFR *R* can be computed, for which the following statements are valid:

i) $J_R = \mu_R - v_R \cdot \mu_R$ is maximal,
ii) The equality $T = R \circ Q$ is retained.

Clearly, this improved version of *R* will be a more significant IFR translating the higher degrees of association and lower degrees of non-association of *J* as well as lower degrees of hesitation to the cost evaluation *C*. If almost equal values for different *C* in *T* are obtained, then we consi- der the case for which hesitation is least. From a refined version of *R* one may

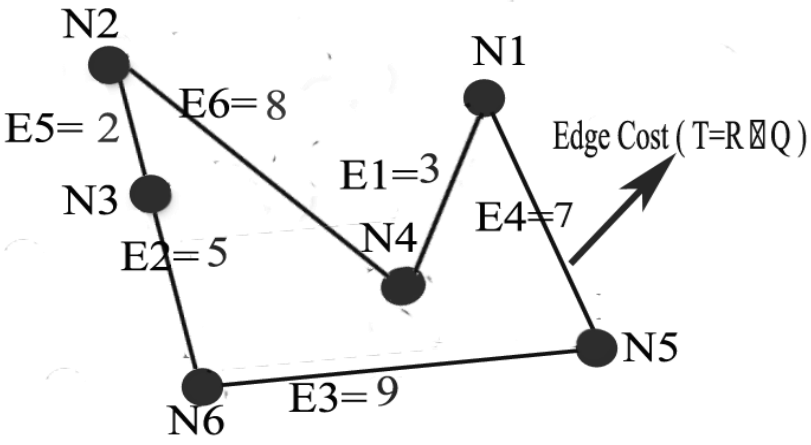

Figure 1. N1, N2, N4, N5, N6.

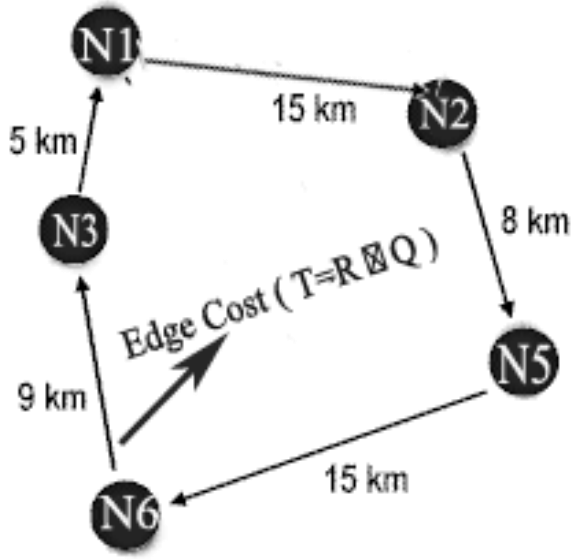

Figure 2. N1, N2, N3, N5, N6.

infer cost from jam factors in the sense of a paired value, one being the degree of association and other the degree of non-association.

APPLICATION ON A SIMPLE TDTSP CASE

Let there be a tour that has only 6 edges (edge 1. – edge 6) as shown in (Table 1). Each edge connects two nodes (Figure 1). Thus, each edge eventually will have a jam cost, depending on the area(s) it crosses. (Table 1) shows each edge and the jam factors associated. The ultimate goal is to be able to calculate the total tour jam factor which will be multiplied in the physical distance between two nodes. Hence, quantifying the jam cost for each edge that is part of that tour path. The intuitionistic fuzzy relation $Q(E \to J)$ is given as shown in (Table 1). Let the set of jam costs be C as in Table 2. The intuitionistic fuzzy relation $R(J \to C)$ as in Table 2. Therefore the composition $T = R \circ Q$ as given in Table 3. We calculate J_R (Table 4). Hence, those numbers quantify the jam factor on each edge.

After a simple calculation

$$(total\ tour\ length\ with\ jam\ factors = edge\ length\ \times \sum_1^M (edge\ jam\ cost),$$

we obtain the actual cost for each tour accumulating the edges after multiplying the physical distances with the jam factors in (Table 4).

Table 1. Route1 = (edge 1, ..., edge 6).

(Q)	Jam area 1	Jam area 2	Jam area 3	Jam area 4
Edge 1	(0,8, 0,1)	(0,6, 0,1)	(0,2, 0,8)	(0,6, 0,1)
Edge 2	(0, 0,8)	(0,4, 0,4)	(0,6, 0,1)	(0,1, 0,7)
Edge 3	(0,8, 0,1)	(0,8, 0,1)	(0, 0,6)	(0,2, 0,7)
Edge 4	(0,6, 0,1)	(0,5, 0,4)	(0,3, 0,4)	(0,7, 0,2)
Edge 5	(0,8, 0,1)	(0,8, 0,1)	(0, 0,6)	(0,2, 0,7)
Edge 6	(0, 0,8)	(0,4, 0,4)	(0,6, 0,1)	(0,1, 0,7)

Table 2. Jam Costs.

Jam area (R)	Cost factor 1	Cost factor 2	Cost factor 3	Cost factor 4
Jam area 1	(0,4, 0)	(0,7, 0)	(0,3, 0,3)	(0,1, 0,7)
Jam area 2	(0,3, 0,5)	(0,2, 0,6)	(0,6, 0,1)	(0,2, 0,4)
Jam area 3	(0,1, 0,7)	(0, 0,9)	(0,2, 0,7)	(0,8, 0)
Jam area 4	(0,4, 0,3)	(0,4, 0,3)	(0,2, 0,6)	(0,2, 0,7)

Table 3. $T = R \circ Q$.

Jam Cost (T)	Cost factor 1	Cost factor 2	Cost factor 3	Cost factor 4
Edge 1	(0,4, 0,1)	(0,7, 0,1)	(0,6, 0,1)	(0,2, 0,4)
Edge 2	(0,3, 0,5)	(0,2, 0,6)	(0,4, 0,4)	(0,6, 0,1)
Edge 3	(0,4, 0,1)	(0,7, 0,1)	(0,6, 0,1)	(0,2, 0,4)
Edge 4	(0,4, 0,1)	(0,7, 0,1)	(0,5, 0,3)	(0,3, 0,4)
Edge 5	(0,4, 0,1)	(0,7, 0,1)	(0,6, 0,1)	(0,2, 0,4)
Edge 6	(0,3, 0,5)	(0,2, 0,6)	(0,4, 0,4)	(0,6, 0,1)

Table 4. Edges Length with Jam Factors.

J_R	Jam cost1	*E* + Jam cost1	Jam cost2	*E* + Jam cost2	Jam cost3	*E* + Jam cost3	Jam cost4	*E* +Jam cost4	*Total Jam Cost/KM*
Edge 1 (3 km)	0,35	1,105	0,68	2,04	0,57	1,71	0,08	,24	5,4
Edge 2 (5 km)	0,20	1	0,08	0,4	0,32	1,6	0,04	0,2	3,2
Edge 3 (9 km)	0,35	3,15	0,68	6,12	0,57	5,13	0,05	0,45	14,85
Edge 4 (7 km)	0,32	2,24	0,68	4,76	0,44	3,08	0,18	1,26	11,34
Edge 5 (2 km)	0,35	0,7	0,68	1,36	0,57	1,14	0,05	0,1	3,3
Edge 6 (8 km)	0,20	1,6	0,08	,64	0,32	2,56	0,04	0,32	5,12
Total Tour Length with jam factors	**Total tour length before jam cost equals 34 km**					**Total tour length after jam cost equals 77,21 km**			

Table 5. Results of graph in Figure 1.

J_R	Jam cost1	*E* + Jam cost1	Jam cost2	*E* + Jam cost2	Jam cost3	*E* + Jam cost3	Jam cost4	*E* +Jam cost4	*Total Jam Cost/KM*
Edge1 (15 km)	0,35	5,25	0,68	10,2	0,57	8,55	0,08	1,2	25,2
Edge2 (5 km)	0,20	1	0,08	0,4	0,32	1,6	0,04	0,2	3,2
Edge3 (9 km)	0,35	3,15	0,68	6,12	0,57	5,13	0,05	0,45	14,85
Edge4 (15 km)	0,20	3	0,08	1,2	0,32	4,8	0,04	0,6	9,6
Edge5 (8 km)	0,20	1,6	0,08	0,64	0,32	2,56	0,04	0,32	5,12
Total Tour Length with jam factors	**Total tour length before jam cost equals 52 km**				**Total tour length after jam cost equals 109,97 km**				

CONCLUSIONS AND FUTURE WORK

In this article, we proposed a novel intuitionistic fuzzy set based model for the realistic extension of the TDTSP, namely, the IFTDTSP model, for considering the jam factors in the original TDTSP problem by applying the IFS theory. Obviously, this improved version will be a more promising approach in translating the higher degrees of association and lower degrees of non-association of jam factor as well as lower degrees of hesitation to any edge's cost and ultimately more realistic calculation for the traveled routes. Our future work will focus on applying the DBMEA meta-heuristics [8, 9] for determining the (quasi) optimal tours (as this algorithm has been repeatedly successfully applied for various NP-hard graph search problems with rather good accuracy, very good predictability and rather universally) to our model and test its efficiency on larger number of nodes.

ACKNOWLEDGMENT

This work was supported by National Research, Development and Innovation Office (NKFIH) K124055.

REFERENCES

[1] Applegate, D.L.; Bixby, R.E.; Chvátal, V. and Cook, W.J.: *The Traveling Salesman Problem: A Computational Study.*
Princeton University Press, Princeton, 2006,

[2] Schneider, J.: *The time-dependent traveling salesman problem.*
Physica A: Statistical Mechanics and its Applications **314**, 151-155, 2002,
http://dx.doi.org/10.1016/S0378-4371(02)01078-6,

[3] Federici, L.; Zavoli, A. and Colasurdo, G.: *A Time Dependent TSP Formulation for the Design of an Active Debris Removal Mission using Simulated Annealing.*
https://arxiv.org/abs/1909.10427, accessed 25th March 2019,

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

[5] Atanassov, R.K.: *Intuitionistic Fuzzy Sets.*
Fuzzy Sets and Systems **20**, 87-96, 1986,
http://dx.doi.org/10.1016/S0165-0114(86)80034-3,

[6] Biswas, R.: *On fuzzy sets and intuitionistic fuzzy sets*.
Notes on IFS **3**(1), 3-11, 1997,

[7] Gau, W.L. and Buehrer, D.J.: *Vague sets.*
IEEE Trans. Systems Man Cybernet **23**(2), 610-614, 1993,
http://dx.doi.org/10.1109/21.229476,

[8] Tüű-Szabó, B. and Kóczy, L.: *Discrete Bacterial Memetic Evolutionary Algorithm for the Time Dependent Traveling Salesman Problem.*
International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems – IPMU 2018. Springer International Publishing, Cham, 2018,

[9] Tüű-Szabó, B.; Földesi, P. and Kóczy, L.: *The Discrete Bacterial Memetic Evolutionary Algorithm for solving the one-commodity Pickup-and-Delivery Traveling Salesman Problem.*
10th European Symposium on Computational Intelligence and Mathematics (ESCIM2018). In press.

Interdisciplinary Description of Complex Systems 18(3), 360-368, 2020

ENVIRONMENTAL SAFETY AND LIVING IN A SMART CITY

Géza Károly Kiss-Leizer*

Óbuda University, Doctoral School of Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.18.3.5
Regular article

Received: 3 March 2020.
Accepted: 1 June 2020.

ABSTRACT

The present study examines the environmental safety and liveability of today's metropolises and cities by discussing the present situation regarding technical sciences, accidents, disasters and waste management, sharing some philosophical thoughts on the future, describing the technical problems, human failures and errors, and finally, by proposing some possible solutions. It is necessary and of upmost importance to address the issues of security, environmental safety and protection, as well as long-term, sustainable liveability of the smart cities of the future by considering the latest technology available today, as proposed in the present study. It outlines some of the guidelines aiming to change human behaviour, the necessity and possibility of ensuring order and eliminating insecurity, chaos and disorder in future smart cities. Furthermore, it wishes to bring attention to the lack and need of scientific research of the elements providing security and liveability of today's cities and metropolises, the absence of which is causing suffering and unbearable living conditions for millions of people. Finally, it proposes an approach of engineering and careful, responsible and forward-looking planning to ensure that people will live in security and dignity in the smart cities of the future.

KEY WORDS

safety science, environmental safety, smart city, environmental protection, coronavirus disease, COVID-19

CLASSIFICATION

ACM: 10010485, 10010554, 10010606
APA: 4070, 4090, 4100, 4140
JEL: L92, O18, R41
PACS: 84.40.Xb

*Corresponding author, η: kissleizer@t-online.hu; +36 30 222 8062;
Budapest, Széchenyi I. u. 9., H–1184, Hungary

INTRODUCTION

People today are primarily interested in obtaining material goods, living in big cities, indulging in a wasteful and senseless manner driven by consumerism, pursuing pleasures instead of natural, environmental or spiritual values. Unfortunately, humans of the present time fail to see and appreciate even their own values and interests, they only live for today and for momentary, cheap and mostly bodily delights.

With a knowledge of thousands of years, we, highly intelligent human beings could do the most for the protection of our environment and cities. First of all, for the Earth, as it should come before Mars, Venus or any other planets with life-supporting conditions in the Universe, which could be conquered and transformed into liveable places where new smart cities can be built. Now, we are destroying the Earth and striving to establish a new life on Mars.

Even if the Earth were not to be saved, or it could not be saved, at least the possibility should be given for a happier, safer life without quarrels, fights, catastrophes and wars.

The processes which are going in the wrong direction, in the background of the development of human societies, are driven by politics, self-interests, lobbying, money and connections.

Our age is ruled by global trends. The divergence of development perspectives, territorial integrity, the unscrupulous morality of fanatic religious leaders, separatism, nationalism, chauvinism, the attacks committed by terrorists hidden in the streets, equipped with bomb belts and clad in black hoods may not only be intimidating, but they can hamper the long-term development of human societies, including the development of environmental security. It is also regrettable that, through national media, these negative influences lacking any moral inhibitions can reach to any depth of the members of the society. The Internet allows the free circulation of any information based on which anybody could create ideologies, bombs, nail-filled pots, magnetic, aluminium-bullet guns, and buy all necessary materials online [1].

Unfortunately, by now environmental protection has become a virtual business, it is all about making money, accelerating consumption and becoming rich.

Table 1. Population city [2].

World population (11 February 2020)	In 2020
Population increase today **103 299** Changes in every 0,38 sec.	Population increase **8 513 336**
Births today **176 621** Changes in every 0,222 sec.	Births **14 556 161**
Deaths today **73 322** Changes in every 0,536 sec.	Deaths **6 042 825**

OBJECTIVES, STATING THE RESEARCH HYPOTHESIS

Cloud-based solutions represent the latest application of complex information technology methods. An important element of ensuring the sustainability of the present systems is increasing their efficiency. For this reason, besides the information and communication technology of cyber space, these systems also depend on technologies with material manifestations. Computing is one of the building blocks of information technology. Therefore, cloud-based computing influences all industries [3].

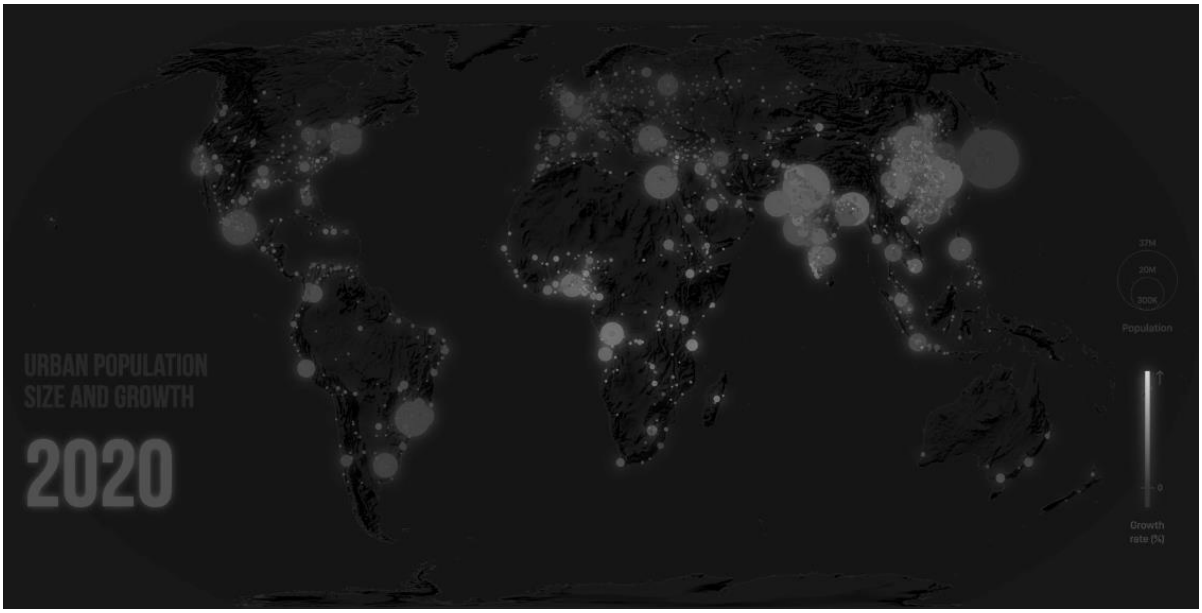

Figure 1. World population today 7.731.881.659 [4].

The interdependencies of systems in smart cities have a significant effect on the operation of the overall system. With the digitalization of the world and the interlocking of different systems, greater attention must be paid to safety and security. The creation of safe societies requires more than ensuring the protection of critical infrastructures [5].

One of the addressed challenges in cities is the transportation of the growing population. Current city transportation systems were implemented with different principles in mind at the time. Due to the development of cities, a public transportation reform is needed as well, so that people could get to their destination safer, faster and easier. The basic concept of designing smart systems is creating a comprehensive, communication-based operation between different units, and this communication ultimately must have a unified format [6].

The serious problems of today's cities call for the creation of safer smart cities in the future. The technologies and technical devices are already available to achieve this objective.

With regard to the applicability of the above-mentioned technologies and devices, this study aims to examine the existence, the present and the future, the operation, lifestyle and liveability or non-liveability of today's megacities, cities and metropolises, by using the latest results of scientific research. If these methods and solutions are applied successfully, they can help to create the smart, safe and liveable cities of the future.

REVIEW OF REFERENCES – WITH REGARD TO THE IMPORTANCE AND RELEVANCE OF THE TOPIC

By the 21st century environmental security has gained a new meaning, sustainability and the protection of natural resources have become an essential element of national security and foreign policy [7].

Certain studies on environmental safety elaborate on ideas according to which environmental problems, especially the shortage of resources and the deterioration of the environment, will lead to violent conflicts between states and societies [8].

A rapidly growing proportion of the world's urban population is now living in megacities. In 1950 there were only two megapolises with more than 10 million inhabitants, New York with a population of 12 million and Tokyo with 11 million people. By 2018, the number of these

metropolises has grown to 33; 20 of which can be found in Asia, 6 in Latin America, 3 in Africa, and 2 in Northern America and Europe respectively. The total of the population living in metropolises is 463 million, which takes 12 % of the global urban population.

According to forecasts, by the year 2035, there will be 48 megacities in the world, most of them in underdeveloped regions. At present Tokyo has the biggest population with 37 million people, followed by (29 million), Shanghai (26 million), Mexico City and Sao Paulo (22 million respectively). Furthermore, there are four megacities with a population of over 20 million. In the following years Tokyo's population will probably decrease, while Delhi's population will increase, so by around 2028, this Indian metropolis will have become the biggest city in the world. In order to achieve the sustainable development objectives for 2030, the successful management of the urbanisation processes of the following decades is of key importance.

The growing of urban population at such a significant rate poses serious problems, especially for less developed countries with a lower income. Adequate housing, infrastructure, public transport and workplaces must be ensured, besides providing wide access to such essential services as public healthcare and education [9].

According to the reports of the Worldwatch Institute**,** we live in a world where 30 % of the population of productive age will not find a job, where 600 million people have no access to healthy drinking water, 1 billion people cannot write or read, 800 million people starve regularly, while, at the same time, 1.6 billion people are overweight. There are 100 million homeless people in the world, 3 million children die each year because of the lack of vaccinations, every year 9 million people and every hour 300 million people die of hunger. At the same time, 2 % of the 1046 billion dollars of the global military expenditures would be enough to provide elementary education, healthcare service, safe drinking water and adequate food for all the people in the world [10].

WASTE MANAGEMENT IN CITY CENTERS

Due to today's preservation procedures, most of our food is over-salted, smoked or contains an excessive amount of preservatives in order to be marketable for a longer period of time. After the expiry date it is to be thrown out, even though it could be used for days, or even for weeks. Similarly to the declaration of consent required in case of certain healthcare treatments, customers should be able to declare that they would buy these products at a lower price on their own risks.

The incredible rate of waste generation must be also mentioned here. In New York, when the supermarkets are closed at 10 p.m., hundreds of black bags are brought out to the street, beside the containers, which are already full. After checking the content of these bags, it turned out that most of them contain one-day old food, especially bakery, which were regarded as unmarketable (while hundreds of millions of people are starving in the world...)

Tens of thousands of rats are feeding on this waste. The attitude of public health authorities is incomprehensible, as tropical rat fleas are the reservoir of pathogenic organisms causing the spread of serious diseases. I did not have to do the shopping for food the next day, beggars do not have to die of hunger, only maybe freeze to death. In San Francisco, I found complete meals in unbroken, original packaging in the bins and next to them.

Unfortunately, the situation in Budapest is becoming similar, as a result of the growing amount of the waste generated, and the irresponsible behaviour of homeless people.

By now, transportation has become the main cause of pollution in cities, before industrial or other causes of pollution. The air and noise pollution caused by transport make cities unliveable. The following map shows the noise pollution in Budapest, which is continuously growing with the increasing number of vehicles.

Figure 2. Strategic noise map of transport in Budapest [11].

It is because of traffic congestions on the roads that people prefer to take the train whenever possible. There are 43 railway stations in Budapest, and it would be possible to get to even the furthest points in 20 minutes much more conveniently, if MÁV (Hungarian State Railways) introduced city shuttle trains using the circular rail, reconstructing the industrial rail tracks and connecting track networks. As the combined season ticket has already been introduced, the question is why these changes have not been made yet.

A major problem is that railway lines in big cities attract homeless people, who live along these lines in railway operating areas. It is difficult to explain how this can be allowed from a railway security perspective. An incredible amount of waste is accumulated by them. The questions should be asked how these areas can be “no-one’s lands”, and why this waste, which is often classified as hazardous, cannot be disposed of (MÁV Department of Environment Protection – Waste Management Group? “MÁV has limited capacities are limited for frequent and costly waste disposal” [12].

The waste generated and carelessly thrown away by canteens, restaurants or kitchens of various institutions must also be mentioned here, as it cannot be used for feeding animals, therefore, it is taken for composting. At the same time, various references on the topic emphasise that cooked food leftovers should not be added to other composted materials.

Figure 3. Litter near main city rail track /Food waste senselessly thrown away.

In the following section, a special case involving hazardous materials will be presented. A railway accident happened in Spain, because the locomotive driver, who was using his mobile phone at the time, failed to notice the posted speed limit of 90 km/h, and entered a bend with a speed of 180 km/h. The locomotive and the following two cars derailed and turned over, several people were seriously injured, and 80 people died. This happened on a railway track with an electric line, where the overhead contact line was missing in a section, so the train was operated by a hybrid electro-diesel locomotive. The diesel engine, which powered the generator to provide electricity for the train, used the diesel stored in the head-end of the train in a tank with a capacity of several thousand litres. Due to the accident, the tank was ripped up, and the diesel escaped. This happened in a city environment, where the water and sewage systems were at a huge risk, as 1 litre of carbon-hydrate fuel can contaminate 1 million litres of water. Still, the most serious consequences were that it caused the death of 80 people.

Figure 4. Railway accident in a Spanish city / HC-polluted bedding.

The photo above on the right was taken at the Western Railway station in Budapest, where long-outdated diesel locomotives pull in, leaving motor oil and lubricant leakages behind. The Danube is 800 meters form here, the flows of groundwater, as our modelling showed, carry the washed-in HC pollution into the river, especially in the periods of low water. This problem could be easily solved by insulating the track sections where diesel locomotives stand, like in the case of landfills, with an HDPE insulation foil, directing rainwater into an oil mud chamber. Such reservoirs are already required by the environmental protection authority for the parking lots for over 10 road vehicles. It should be introduced in this case, too (MÁV Department of Environmental Protection – Waste Management Group – Environmental Protection Agency).

The cleaning of the railway track bedding and its environment from the pollution caused by the leakage of hazardous materials requires huge and costly earth moving and other work. Furthermore, the transportation and disposal of such polluted materials is also very expensive. Compared to this, the cost of fuel loss is rather insignificant [1].

The cargo must be secured, because the cargo itself could be endangered, or it may pose a threat to the environment. Therefore, protection and defence are of key importance to keep the cargo safe. Guarding is a permanent counteraction responding to a presumed threat on the cargo. The guard so an insurance one attaching to a hypothetical, supposed activity, the protection it began though, a related averting task ensued with an event concerned. A large amount of waste is expected to be generated in case of rail disasters. The decontamination and disposal of such waste – polluting soil or water – is an urgent objective, as well as the elimination of the pollution and the rehabilitation of the affected area [13].

It is important to highlight the significance of hydrocarbons polluting the soil and water ecosystems. These chemicals are released into the environment as the products of combustions, or due to accidents or disasters. The effects of liquid hazardous materials of industrial origins

must also be mentioned here. Today, it is a great challenge to address the threats posed by such liquid materials, as these substances can easily become hazardous wastes once they escape [14].

In addition, train cars with open toilet bowls should be replaced by ones fitted with a closed toilet system. Faeces, often carrying infections, fall onto the railway track and wash into ground water, or fall directly into living waters from bridges. The attitude of public health authorities is inexplicable: “462 vehicles of MÁV Start Zrt. have closed toilet facilities, that is 18 per cent of the vehicles. All newly procured vehicles are equipped with such closed-system toilets. The last vehicles with an open toilet system will be withdrawn from service in 15-20 years”. This issue cannot wait that long.

Figure 5. US train toilet at Amtrak/The emptying of closed train toilets at a station.

Another problem is that public toilets have been closed down in cities as shops or bars have taken their places. People then relieve themselves in public areas. Again, the responsibility of public health and other authorities should be emphasised here, in order to ensure hygene and public morality, educate children, avoid epidemics, among various other reasons.

Today’s megacities are called ‘the ulcers of the Earth’, which reflects the quality of everyday life of the people living in such cities. Still, millions are moving into megapolises, where no silence or peace can be found, only frantic rush, stress and the constant flow of vehicles and people in the streets.

The great Italian musician Nini Rosso wrote the song called Il Silentio - the sound of silence. Small villages can show us examples of how to find peace and quiet, but unfortunately, they cannot offer job opportunities, therefore, a growing rate of the Earth’s population opt for unliveable cities with all their filth and suffering.

DISCUSSION

When identifying the relationship between the critical risks of great cities, the first step to be taken is to elaborate a holistic approach and the future perspective of critical infrastructures, and to transform them into a collective value.

Critical infrastructures can be defined as the network of interrelated, interactive and interdependent infrastructural elements, facilities, services, systems and processes which are essential for the operation of a country (its public, economy and government), and have a crucial role in ensuring the socially required minimum level of legal certainty, public order, national security and economic operability, and in maintaining secure public health and environmental conditions.

A holistic approach means that emerging problems should not be addressed individually, as they occur in a system and they relate to each other in various ways, as the result of globalization. This holistic approach demands the reconciliation of short-term and long-term, as well as local and global interests, and the application of precautionary and subsidiarity principles.

Due to the adverse processes in today's great cities, it is necessary to revise and redefine public health and environmental security, in order to prevent and eradicate epidemic diseases spreading fast between cities. In 2019, a highly pathogenic coronavirus strain appeared in Wuhan, the most populated city of Central China. As a result of free mobility and social relations, the virus has spread at an incredible rate, causing a pandemic in all the countries of the world.

In the ecosystem, from the beginning of time and from the first steps of evolution, all living organisms have a natural enemy, like immunity, the protective system of the host against bacteria and viruses. This continuous change happens from one extreme to the other, the light and shadow alternating constantly, according to the ancient principles of living in good health and surviving diseases.

In the course of epidemic-related research, it could be taken into consideration that 1 kilogram of forest soil contains billions of living microorganisms, and if it is reacted with the coronavirus in physiological solution, it is possible to find a microorganism which is the natural enemy of the coronavirus. As opposed to the function of the bacteriophage, in this case it is not the bacteria that could be killed, but the bacteria would kill the virus with its toxin or by a process not yet known. It is also possible that the enzymes of the protozoa (microscopic single-celled eukaryotes) might offer the right solution. It cannot be excluded that something else would bring the solution from the microorganisms. This way the appropriate protection against the coronavirus could be ensured by finding an effective antidote.

Burying our head in the sand and sitting at home cannot be the right solution! The American movie "Independence Day" shows an example how intruders can be destroyed (with the help of a computer virus), We, people of the world must join our forces and fight to destroy this virus by any weapons or by any means, once and for all, as we did with the plague and the cholera. This virus is a living organism, if it is vulnerable, it is also destroyable (the American movie "Predator").

In this case too, a holistic approach is needed in order to delay the pandemic and to eliminate it finally. Therefore, such measures must be introduced which ensure the identification of the effective ways of protection, the further risk assessment, the definition, selection and ranking of counter measures and public health – epidemiological activities. This could be a major scientific result, which guarantees the protection of the population of future smart cities against harmful pathogens.

SUMMARY

The aforementioned and discussed problems, related to the smart cities of the future, can be addressed with adequate solutions that are already available today.

The main objective is to ensure that cities become noise-free, clean and altogether liveable places to inhabit. In order to achieve this goal, the present level of excessive consumerism must be lowered, and the use of resource-wasting production methods as well as the related release of hazardous materials must be ceased. City slums, litter dumps, pests, homeless people living in the streets, noise, air and light pollution must also be eliminated. Moreover, the luxurious and privileged lifestyle established and pursued by the rich must be abandoned. Resources and natural assets must be distributed and used on the principles of fairness and sustainability among all humans.

For all these changes to be accomplished, first a holistic approach and vision must be developed and turned into a collective value. Hunger, misery, insecurity, desperation and criminality must be ended, while healthy living conditions, drinking water, food, housing and education must be provided by transferring all our knowledge.

Decision makers and executives must be accounted for the billions spent senselessly, armaments must be stopped as well as all terror acts, wars and violence.

The values and natural assets represented by city environments must be used to fulfil economic and social needs in a way which, instead of promoting consumption at all costs, or expecting a return on invested capital, prioritizes careful and forward-looking environmental engineering and the long-term sustainability of the environment.

By understanding Earth system processes, and by careful, responsible and progressive engineering, safe and humane living conditions can be achieved in smart cities.

REFERENCES

[1] Kiss-Leizer G.K.: *A Brief History and Interpretation of Environmental Safety.*
Safety and Security Sciences Review **1**(3), 35-47, 2019,

[2] –: *Population City.*
http://nepesseg.population.city/world, accessed 11th February 2020,

[3] Albini, A. and Rajnai, Z.: *General Architecture of Cloud*.
Procedia Manufacturing **22**, 485-490, 2018,
http://dx.doi.org/10.1016/j.promfg.2018.03.074,

[4] Visual Capitalist: *Map global rise of urbanization*.
https://www.visualcapitalist.com/map-global-rise-of-urbanization/, accessed 11th February 2020,

[5] Tokody, D. and Schuster, G.: *Driving Forces Behind Smart City Implementations – The Next Smart Revolution*.
International Journal of Emerging Research and Solutions in ICT **1**(2), 1-16, 2016,

[6] Tokody, D. and Mezei, I.J.: *Creating smart, sustainable and safe cities.*
Proceedings of the 13th IEEE International Symposium on Intelligent Systems and Informatics.. IEEE, Subotica, 000141-000146, 2017,

[7] Butts, K.H.; Goodman, S. and Nugent, N.: *The Concept of Environmental Security*.
Solutions **3**(1), 55-56, 2012,
http://dx.doi.org/10.1111/j.1439-0507.2012.02204.x,

[8] Swatuk, A.L.: *Environmental security in practice: transboundary natural resources management in southern Africa.*
Pan-European Conference on International Relations, 9-11 Sept., 2004. The Hague, 2004,

[9] KSH: *Statistical mirror World Population Day.*
http://www.ksh.hu, accessed 1st February 2020,

[10] –: *Situation of the World*.
https://www.vilaghelyzete.com/2019, accessed 14th February 2020,

[11] Budapest: *Environmental Protection.*
https://geoportal.budapest.hu/Kornyezetvedelem/ZAJ/2007/Agglo, accessed 12th February 2020,

[12] MÁV Service Center Ltd.: *Hulladékgazdálkodás*.
https://www.mavcsoport.hu/mav-szk/hulladekgazdalkodas, accessed 18th February 2020,

[13] Kiss-Leizer, G.K.: *Possible areas of application of drones in waste management during rail accidents and disasters.*
Interdisciplinary Description of Complex Systems **16**(3-A), 360-368, 2018,
http://dx.doi.org/10.7906/indecs.16.3.8,

[14] Kiss Leizer, G.K. and Pokorádi, L.: *Waste Management Issues in Air Transport*.
Aeronautics Publications **27**(2), 17-25, 2015,
http://dx.doi.org/10.12968/eyed.2015.17.5.25.

Interdisciplinary Description of Complex Systems 18(3), 369-374, 2020

ADAPTATION OF CLOUD THEORY IN THE INFOCOMMUNICATION SYSTEM OF AUTONOMOUS VEHICLES

Attila Albini*, Dániel Tokody and Zoltán Rajnai

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.18.3.6
Regular article

Received: 3 March 2020.
Accepted: 28 May 2020.

ABSTRACT

Transport infrastructures are part of the global transport architecture. The operation of each nation's transport infrastructure is essential for the sustainability of national economies. Therefore, these systems are considered as critical infrastructures from the perspective of national security. It is understandable that smart mobility is one of the indicators of the smart city concept. An important element of the transportation system is the IT infrastructure, which is connected to the local systems of smart cities. In the system of a smart city the central management subsystem is the server component and the moving objects are the client devices. Autonomous vehicles can obtain the information they need for transport from their on-board equipment, from the central control of the smart city or from each other. The most important requirement of the autonomous vehicle's own system is high availability with adequate performance. For this reason, it is worth examining the applicability of availability-enhancing technologies in these vehicles. This article examines the adaptations of the cloud system requirements and cloud building technologies in the infocommunication system of autonomous vehicles.

KEY WORDS

cloud requirements, cloud building technology, adaptation, autonomous vehicles

CLASSIFICATION

ACM: K.6.5, C.0
JEL: R41, O39

*Corresponding author, η: attila.albini@gmail.com; +3630 526 7757;
OE-BDI office, Nepszinhaz str. 8, 1081 Budapest, Hungary

INTRODUCTION

An important requirement for existing systems is sustainability. The smart city concept has evolved as a result of sustainability. The core infrastructure is the basis of the smart city model, which incorporates infocommunication technology in accordance with modern requirements [1]. The model groups the resource elements that are the indicators of habitat sustainability. This model is one of the technologies determining the near future, and is therefore an important element of both R&D [2] and education [3, 6].

Smart mobility is an indicator of the smart city concept [7]. Central regulatory systems are essential for smart mobility. In the model, mobile units (autonomous vehicles) are considered as the local elements. Local mobile elements can acquire information by interpreting their environment, from the central components and from each other. The autonomous vehicle system makes decisions [8, 9] based on the information thus obtained. In this model IT problems are augmented by the system of control [10-13], which is usually implemented by IoT devices.

This study with a service-centered approach examines the problems related to the infocommunication systems of autonomous vehicles on philosophical foundations. This way the research is based on a unified method. Furthermore, it provides an opportunity to adapt solutions to similar problems related to cloud building technologies in the infocommunication system of autonomous vehicles.

PROBLEMS OF THE ICT SYSTEM OF AUTONOMOUS VEHICLES

Organizing problems around philosophical questions unifies the methods of investigation. The main philosophical issues and the related problems are as follows [14]:

- existence problem: the equivalent of examining the long-term existence of things. This is the issue of high availability. This problem occurs in practice for all vital elements. For example, positioning, keeping the vehicle on the track, brake assistance, other safety features,
- knowledge problem: the equivalent of knowing the structure of things. This is necessary to achieve a flexible structure, which is an issue of the IT architecture. As a practical problem, parts of the vehicle's infocommunication system may not be interchangeable, so a complete subsystem may need to be redesigned and implemented,
- the problem of action: the equivalent of the functionality of things. The question of performance is relevant here, and response time is the most important parameter. This problem is relevant to all solutions that require large amounts of data to be processed. The security features mentioned above can also be mentioned: positioning, keeping the vehicle on the track, brake assistance,
- the problem of truth: the equivalent of the validation, control and response to environmental changes. This models the operation of the system without an organic change. The most important aim is to make a prompt decision. This problem is relevant to all solutions that are for safety and require large amounts of data to be processed,
- change management: the equivalent of the study of the long-term sustainability of the system, which includes organic changes [15-17]. Currently automating organic change is not in the scope for smart systems.

THEORETICAL SOLUTIONS IN CLOUD SYSTEMS

Problems similar to those mentioned above also appear in general infocommunication systems. Solutions to problems with general purpose systems led to the development of cloud technology. Accordingly, the features of infocommunication clouds include high availability flexible architecture, which together with full control allows for adequate performance and response time. The technologies used to build infocommunication clouds are as follows [18]:

- cluster technology ensures high availability through the distribution of tasks,
- grid technology is also based on the division of tasks, but its main purpose is to speed up processing, which ensures fast response time,
- split technology for disaster tolerance,
- virtualization provides flexibility and layered architectural independence.

All these technologies can achieve the required availability and performance. This way they can offer an answer to the problems of the infocommunication system of autonomous vehicles. However, these technologies also serve to enhance IT security [19-21]. Increasing IT security also implies the security of transported people [22]. Therefore, in the case of autonomous vehicles, the issue of IT security is closely linked to the issue of physical security [23-25].

ADAPTATION OF SOLUTIONS

The adaptation of infocommunication cloud solutions requires that the autonomous vehicle infocommunication architecture is similar to the cloud architecture [26]. To achieve this, one should build the following layer structure:

- the energy layer converts natural resources into physical infocommunication resources for infocommunication devices,
- the hardware layer transforms the physical infocommunication resources into logical infocommunication resources,
- the virtualization layer reorganizes the logical infocommunication resources in the manner and to the extent necessary for the operational layer,
- the operational layer creates the desired services using the energy provided by the logical infocommunication resources,
- the management layer provides control over time operation.

The energy, hardware and management layers of the structure to be developed may be the same as those of other vehicles, provided they meet reliability requirements. However, it is worthwhile designing virtual and operational layers, so that physical devices and infocommunication services are separated, and the cloud technologies used to solve the problems are applied between the two. Accordingly, the two affected layers also perform the following virtual functions (Figure 1.):

- resource virtualization,
- application of cloud technology solutions:
  - grid technology
  - cluster technology
  - split technology
- service virtualization

CONCLUSIONS

Sustainability efforts have resulted in the creation of a smart city model. One of the indicators of the smart city concept is smart mobility [7]. The local components of smart mobility are the autonomous vehicles. The problems of autonomous vehicles are worth discussing on a philosophical basis. It allows us to adapt unified solutions from other areas.

Philosophical topics are organized around issues of existence, knowledge, action, truth and change [14]. As a result, the infocommunication problems of autonomous vehicles are related to availability, flexible architecture, performance and control. In general-purpose IT systems,

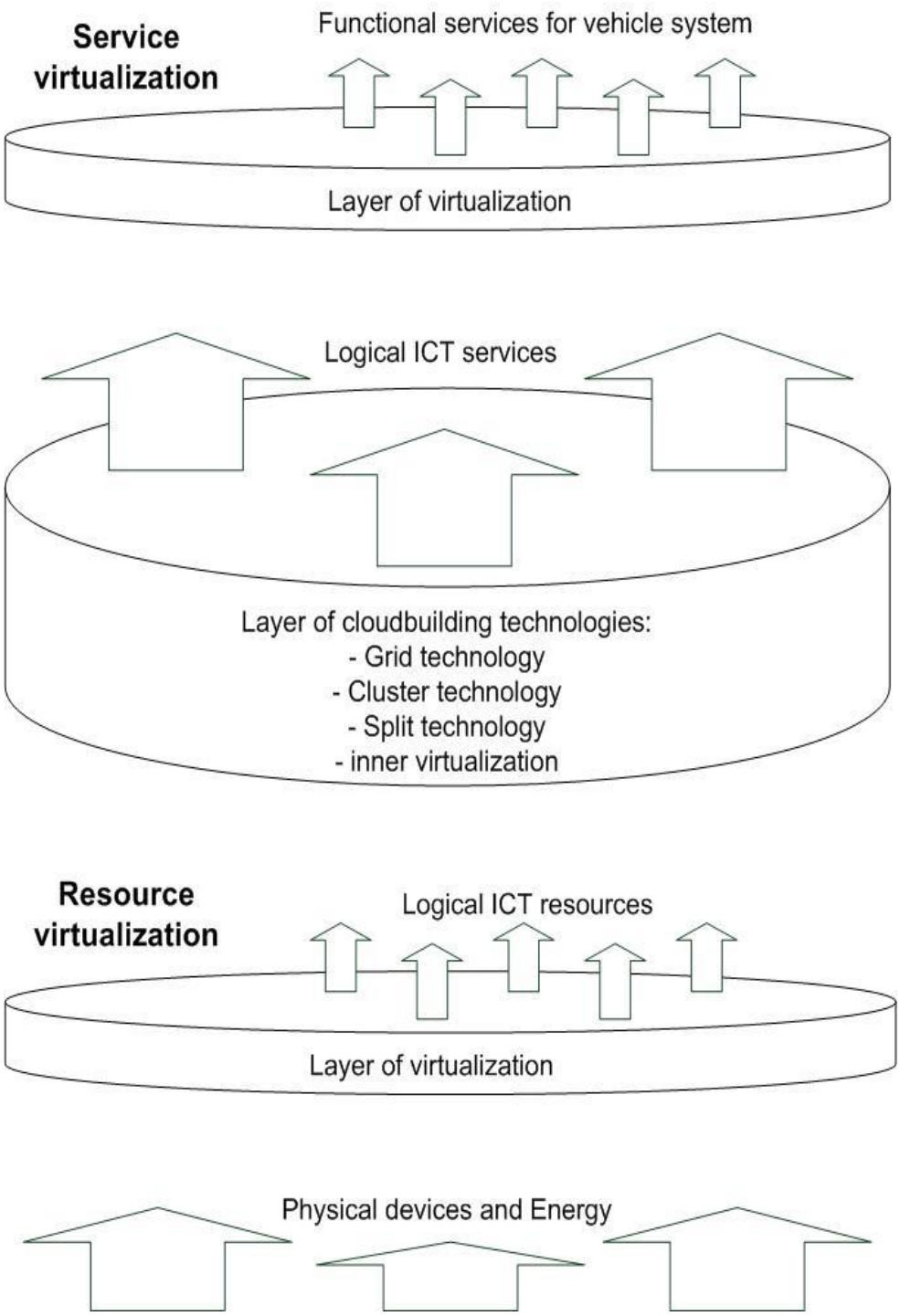

Figure 1. Cloud technologies in the ICT layers of vehicles.

solving similar problems has led to the emergence of infocommunication clouds [18]. Therefore, it is worth exploring the applicability of cloud technologies in autonomous vehicle systems.

The research shows that the structure of the infocommunication system of autonomous vehicles could be designed according to the structure of general infocommunication systems. This is how cloud technologies can be applied. The layers to be created include the energy layer, the hardware layer, the virtualization layer, the operational layer and the management layer [26]. In order to solve the discovered problems, the virtualization layer and the operational layer should be designed so that physical resources are covered from the lower layers, and only the end services are visible to the upper layers, while cloud technologies are applied in these two layers.

ACKNOWLEDGEMENTS

The research presented in this article was carried out as part of the EFOP-3.6.2-16-2017-00016 project in the framework of the New Széchenyi Plan. The completion of this project is funded by the European Union and co-financed by the European Social Fund.

REFERENCES

[1] Tokody, D.: *Digitising the European industry - holonic systems approach*.
Procedia Manufacturing **22**(2018), 1015-1022, 2018,
http://dx.doi.org/10.1016/j.promfg.2018.03.144,

[2] Rodic, A.; Jovanovic, M.; Popic, S. and Mester, G.: *Scalable Experimental Platform for Research, Development and Testing of Networked Robotic Systems in Informationally Structured Environments*.
Symposium Series on Computional Intelligence, Workshop on Robotic Intelligence in Informationally Structured Space, In: *Proceedings of the IEEE SSCI 2011*, Paris, 136-143, 2011,

[3] Szabó, A.; Szucs, E. and Berek, T.: *Illustrating Training Opportunities Related to Manpower Facility Protection through the Example of Máv Co.*
Interdisciplinary Description of Complex Systems **16**(3-A), 320-326, 2018,
http://dx.doi.org/10.7906/indecs.16.3.3,

[4] Mester, G.: *Rankings Scientists, Journals and Countries Using h-index.*
Interdisciplinary Description of Complex Systems **14**(1), 1-9, 2016,
http://dx.doi.org/10.7906/indecs.14.1.1,

[5] Dobrilovic, D. and Odadzic, B.: *Virtualization Technology as a Tool for Teaching Computer Networks.*
International Journal of Educational and Pedagogical Sciences **2**(1), 41-45, 2008,

[6] Mester, G.: *Academic Ranking of World Universities 2009/2010.*
Ipsi Journal, Transactions on Internet Research, TIR **7**(1), 44-47, 2011,

[7] Tokody, D.; Schuszter, G. and Papp, J.: *Study of How to Implement an Intelligent Railway System in Hungary*.
In: Szakál, A., ed.: SISY 2015: *IEEE 13th International Symposium on Intelligent Systems and Informatics: Proceedings*, IEEE, New York, 2015,

[8] Mester, G.; Pletl, S.; Nemes, A. and Mester, T.: *Structure Optimization of Fuzzy Control Systems by Multi-Population Genetic Algorithm*.
In: *Proceedings of the 6th European Congress on Intelligent Techniques and Soft Computing*, Aachen, pp.450-456, 1998,

[9] Zamfirescu, C.B.; Duta, L. and Iantovics, L.B.: *The Cognitive Complexity in Modelling the Group Decision Process.*
BRAIN Broad Research in Artificial Intelligence and Neuroscience **1**(2010), 69-79, 2010,

[10] Mester, G. and Rodic, A: *Sensor-Based Intelligent Mobile Robot Navigation in Unknown Environments*.
International Journal of Electrical and Computer Engineering Systems **1**(2), 1-8, 2010,

[11] Mester, G. and Rodic, A.: *Simulation of Quad-rotor Flight Dynamics for the Analysis of Control, Spatial Navigation and Obstacle Avoidance*.
In: *Proceedings of the 3rd International Workshop on Advanced Computational Intelligence and Intelligent Informatics* (IWACIII 2013), Shanghai, pp.1-4, 2013,

[12] Mester, G.: *Obstacle Avoidance and Velocity Control of Mobile Robots.*
In: *Proceedings of the 6th International Symposium on Intelligent Systems and Informatics SISY 2008*. IEEE, Subotica, pp.97-101, 2008,

[13] Mester, G.; Pletl, S.; Pajor, G. and Basic, D.: *Adaptive Control of Rigid-Link Flexible-Joint Robots*.
In: *Proceedings of 3rd International Workshop of Advanced Motion Control*, Berkeley, pp.593-602, 1994,

[14] Albini, A.; Mester, Gy. and Iantovics, B.L.: *Unified Aspect Search Algorithm*.
Interdisciplinary Description of Complex Systems **17**(1-A), 20-25, 2019,
http://dx.doi.org/10.7906/indecs.17.1.4,

[15] Albini, A. and Rajnai, Z.: *Modeling general energy balance of systems.*
Procedia Manufacturing **32**(2019), 374-379, 2019,
http://dx.doi.org/10.1016/j.promfg.2019.02.228,

[16] Kasac, J.; Stefancic, H. and Stepanic, J.: *Comparison of social and physical free energies on a toy model.*
Physical Review E **70**(1), 16117-16124, 2004,
http://dx.doi.org/10.1103/PhysRevE.70.016117,

[17] Albininé Budavári, E. and Rajnai, Z.: *The Role of Additional Information in Obtaining information*.
Interdisciplinary Description of Complex Systems **17**(3-A), 438-443, 2019,
http://dx.doi.org/10.7906/indecs.17.3.2,

[18] Albini, A; Tokody, D. and Rajnai, Z.: *Theoretical Study of Cloud Technologies.*
Interdisciplinary Description of Complex Systems **17**(3-A), 511-519, 2019,
http://dx.doi.org/10.7906/indecs.17.3.11,

[19] Kiss, M.; Breda, G. and Muha, L.: *Information security aspects of Industry 4.0*.
Procedia Manufacturing **32**(2019), 848-855, 2019,
http://dx.doi.org/10.1016/j.promfg.2019.02.293,

[20] Kovács, Z.: *Cloud Security in Terms of the Law Enforcement Agencies.*
Hadmérnök **7**(1), 144-156, 2012,

[21] Szabó, Z.: *The effects of globalization and cyber security on smart cities*.
Interdisciplinary Description of Complex Systems **17**(3-A), 503-510, 2019,
http://dx.doi.org/10.7906/indecs.17.3.10,

[22] Tokody, D. and Flammini, F.: *Smart Systems for the Protection of Individuals.*
Key Engineering Materials **755**(2017), 190-197, 2017,
http://dx.doi.org/10.4028/www.scientific.net/KEM.755.190,

[23] Pető, R.: *Security of Smart City.*
Interdisciplinary Description of Complex Systems **17**(1), 13-19, 2019,
http://dx.doi.org/10.7906/indecs.17.1.3,

[24] Shatnawi, M.M.: *Applying Information Security Risk Management Standards Process for Automated Vehicles*.
Bánki Reports **2**(1), 70-74, 2019,
http://dx.doi.org/10.1111/oli.12220,

[25] Hell, P.M. and Varga, P.J.: *Drone systems for factory security and surveillance*.
Interdisciplinary Description of Complex Systems **17**(3-A), 458-467, 2019,
http://dx.doi.org/10.7906/indecs.17.3.4,

[26] Albini, A. and Rajnai, Z.: *General Architecture of Cloud*.
Procedia Manufacturing **22**(2018), 485-490, 2018,
http://dx.doi.org/10.1016/j.promfg.2018.03.074.

Interdisciplinary Description of Complex Systems 18(3), 375-381, 2020

SENSITIVITY ANALYSIS FOR CONDOMINIUM LIGHTNING PROTECTION RISK ANALYSIS

Zoltan Kasza*

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.18.3.7
Regular article

Received: 17 February 2020.
Accepted: 23 June 2020.

ABSTRACT

Today we live in an accelerated world. In our environment there are more facilities to serve our needs than ever before, and today's devices have multiple functions, and probably they will gain new functions as well. They are called smart devices. Smartphones, tablets, smart TV-s and potential smart vehicles will create a new environment. As a result of the continuous development of human living communities (villages, towns and settlements), the dominant usage of smart tools and technologies already represents a new quality level (Smart City). These new devices require a new level of lightning protection. Natural forces endanger buildings as well as human lives. The protection of artificially created objects and of the built environment has always played a prominent role, and nowadays, one of its main areas is the lightning protection of structures. The calculation of the lightning protection is based on the MSZ EN 62305 [1] standard. In the past, several changes were made in the standards and decrees [2], and now the current standard is the MSZ EN 62305. It contains the exact mathematical methods of risk assessment using the parameters of buildings and their installations (e.g. lightning protection installations, cables, flooring etc.). The present research aims to identify the relationships between output parameters determined by the input parameters based on the current standards, and the identification of risks by their analysis in different types of buildings.

KEY WORDS

structure safety, lightning protection, risk analysis, safety instructions, sensitive check

CLASSIFICATION

ACM: 10002978.10003029
JEL: D81, C61

*Corresponding author, η: kaszazoltan81@gmail.com; -;
1034 Budapest, Bécsi str. 96/b, Hungary

INTRODUCTION

Natural forces endanger buildings and human lives. The protection of artificially created objects has played a prominent role, and nowadays one of its main areas is the lightning protection of structures. When Benjamin Franklin invented the first lightning rods [3], people started to protect their structures against lightning strikes. Nowadays, based on the observation of natural phenomena, it can be concluded that due to the global warming caused by infrastructural activities, the number of lightning strikes has increased. As much as 1 % of temperature rise will increase the number of lightning strikes by 6 % per annum [4]. Lately, new standards have been issued with the collection of rules on designing lightning protection for buildings. The lightning protection systems of buildings are designed and implemented for the protection of human lives and property. The scope of the present research is to prioritize input parameters for the lightning protection risk management of buildings for different common structures (e.g. condominiums, hospitals, schools, etc.). It is based on the risk computing IT program the author has written. This program calculates the lightning protection risk components using the current standard's calculation method and then aggregates them.

Today many people believe that it is enough to protect against lightning with a lightning rod. Indeed, 50-100 years ago this was enough. The reason is that at that time electrical equipment was quite simplistic compared to the present, and it needed special protection on a very basic technical level. However, today the lightning rod alone is not enough. During that time, lightning protection was enough against fire protection, but as mentioned above, now there are new (sensitive) electrical devices which need a "new" type of protection. This protection is against the secondary effect of lightning strikes [5]. So, this external protection against fire is not enough anymore because of the need for the individual protection of electrical devices and equipment inside the building [6]. While in the past our environment consisted of relatively few components (e.g.: building, heating system, energy supply), by now our artificial environment has become much more complex, thus making lightning protection risks more complex. The earlier standard, with its simpler calculation methods, kept pace with the state-of-the-art and technological development for some time, but after a while it was no longer suitable for this purpose, so MSZ EN 62305 came into force.

INTRODUCTION OF THE SCIENTIFIC PROBLEM

There are 58 parameters for calculating risk. When the building is complex, a large number of parameters has to be taken into account. In addition, the development of lightning protection is becoming more complex. The high number of parameters can also make the design and construction of the lightning protection system of the building considerably more difficult, therefore, knowing the priority order of the existing unique parameters specific to the given building can reduce its complexity.

During the process of risk assessment and the development of lightning protection, it was doubted whether all parameters have the same effect on the result. The present research has a practical benefit. When the building is in the design phase and its lightning protection is being designed, the use of visible solutions for lightning protection, which are almost irreplaceable afterwards, can be avoided.

This research on the lightning protection risk analysis of buildings wishes to identify general and specific parameters and their changes.

During the calculation of risk assessment, the following topics were set up to do this research:

- Grouping of input parameters into strong[1] and not strong groups.
- Identification of extremely strong[2] parameters in strong group.

Due to some co-areas, some other questions arose. This research can be completed with the following topics:

- Lightning protection for non-metallic body vehicles.
- Detection of possible shortcomings in the future draft standards.

The present research aims to achieve the first objectives. Details and other topics will be presented in the final dissertation.

QUESTIONS ABOUT THE RESEARCH

Research questions were set up during the risk assessment of different buildings. The questions and ideas were raised during the calculation and some practical development processes.

RQ_1: Not all input parameters can affect output equally (so can they be grouped into strong and not strong categories?).

RQ_2: If **RQ_1** is answere positively, can some parameters be identified as priority within a strong group?

RQ_3: Do the parameters categorized as strong and not strong in the current standard match the strong and not strong grouping of future parameters in the standard?

RISK CALCULATION METHOD

The present research will be based on the calculation of the standard. The lightning protection requirements and the calculation for buildings are contained in the standard MSZ EN 62305 [1], which currently consists of four parts (Figure 1). The specific risk calculation method is described in document 62305-2.

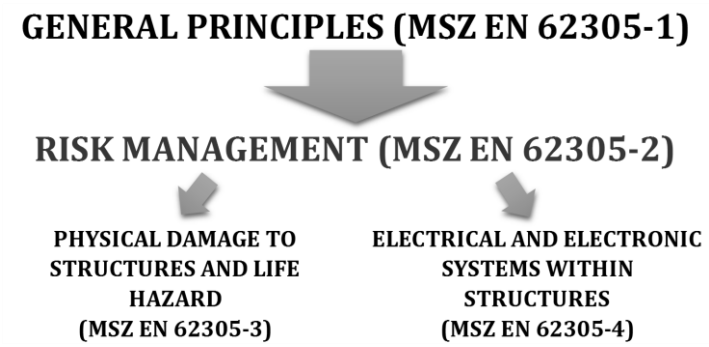

Figure 1. MSZ EN 62305 Standard family [1].

The standard defines four possible risks for lightning strikes:

Table 1. Types of risks [1].

Risk symbol	Risk description
R_1	Risk of loss of human life (including permanent injury)
R_2	Risk of loss of service to the public
R_3	Risk of loss of cultural heritage
R_4	Risk of loss of economic value

The present research will focus on the risk of the loss of human life (R_1).

The standard defines four possible points for the location of a lightning strike (Table 2 and Figure 2) [1]:

Table 2. Types of sources [1].

Source symbol	Source description
S1	Flashes to a structure
S2	Flashes near a structure
S3	Flashes to a line
S4	Flashes near a line

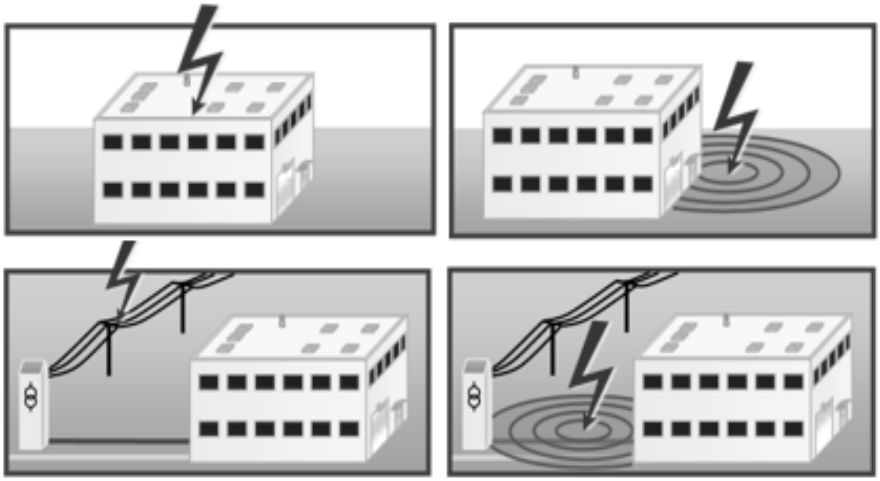

Figure 2. Possible sources of lightning [7].

The calculation of risk is specifically included in the standard. The standard defines a building as legally protected if the calculated risk (R_1 , R_2 , R_3 , R_4) is less than the officially stated value (R_T) in the standard. An exception is the risk of public service disruption (R_2), where the National Fire Protection Code (OTSZ[3]) [8] required a stricter reference value than R_T, but it returned to the standard value from 2020 January. In technical terms, there is always a residual risk. The risk calculation takes into account the parameters of the building and its installations (e.g. the lightning protection of structures, cables, floors, etc.). The result of the risk calculation (R_1) gives a value whether the tested building is protected against lightning or not. This parameter R_1 is the sum of the partial results R_A, R_B, R_C, R_M, R_U, R_V, R_W and R_Z. If the value is less than or equal to $R_T = 10^{-5}$ ($R_1 = < R_T$), then the building can be considered lightning protected. If it is greater than 10^{-5}, lightning protection measures are required. The result of the risk calculation shows whether the building is legally protected from lightning protection or not. If the result shows that it is not, further lightning protection measures must be taken and the calculation must be performed again. If the result is repeatedly "unprotected" then the lightning protection measures must be improved until the result is "protected". In many cases, for the sake of transparency, the result obtained is compared to $R_T = 10^{-5} = 100$ %, so the percentage of the result obtained.

The risk of losing human life (R_1) consists of 8 parts. The risk of losing R_1 human life can be calculated by adding up these partial calculations:

$$R_1 = R_A + R_B + R_C + R_M + R_U + R_V + R_W + R_Z. \quad (1)$$

The partial calculations of the standard use the multiplication method of

$$R_X = N_X \times P_X \times L_X,$$

where N_X is number of dangerous events per annum, P_X – probability of damage to a structure and L_X – consequent loss.

Defined as components of R_1: x ϵ {A, B, C, M, U, V, W, Z}

This short example shows some main parameters of a building, and the R_1 result:

Dimensions of building:	L,W,H = 30 m ; 20 m ; 20 m
Lightning strike number per annum:	$N_G = 2$
Structure location factor:	$C_D = 1$
LPS[4] level:	LPS = II
Length of power line:	$L_L = 200$ m
Type of power line:	Buried → $C_I = 0,5$
Length of telecommunication cable:	$L_L = 100$ m
Type of telecommunication cable:	Buried → $C_I = 0,5$
Material of floor	Wooden → $r_{ta} = 10^{-5}$
Material of ground around building	Grass → $r_{tu} = 10^{-2}$
Factor reducing loss depending on risk of fire	$r_f = 0,1$
Factor reducing the loss due to provisions against fire	$r_p = 0,5$
Number of people in zone	$n_{z1} = 100$ persons
Number of people in front of building	$n_{z2} = 15$ persons
Total number of people	$n_t = 15 + 100 = 115$ persons

$R_1 = 0,8524 \times 10^{-5}$
Because $R_T \geq R_1$ → building protected

The Sensitivity test targets to analyse the effect of single unit changes in the input parameters being examined on the output. There are two types of input parameters (independent variables). One has fixed values defined in the standard, and the others have variable values. These are parameters about lengths. During the test, a change in the value of an input parameter at a time is used to determine the output change, examined separately for each input parameter. At the end of the test, it can be seen whether there is a parameter (strong parameter) which, with a small change in its value, will have a decisive influence on the value of the output (R_1) lightning protection risk. The present research was performed with the program written by the author.

RESULT OF THE TEST

After finishing the sensitivity check, it can be expected that the input parameters can be grouped into strong and not strong parameters, respectively. Strong parameters should be able to identify an extremely important factor that has a decisive influence on the output. If the strong parameters and the 'weak points' of the building are known, the lightning protection engineer can make suggestions to the architect to change or install parts or components, which will no longer be possible once the construction has begun. There are several options to consider before the construction begins. One option is the use of a grounding net, which must be installed in the ground. It is also economically useful to know the parameters beforehand. Another example is the type of the roofing material. Lightning protection is decisively influenced by the type of the roofing material, so it is possible to decide before the construction that the roof will not be made of a combustible material (e.g. sandwich panel) but rather of a more expensive but non-combustible rock wool.

After finishing the sensitivity test, it has been found that unit changes for the input parameters do not affect the output R_1 (lightning protection risk) in the same way. A group of the so-called weak parameters has a minimal effect or nothing on the R_1 output, which stays below the tolerated value $R_T = 1 \cdot 10^{-5}$. On the other hand, five parameters have been identified, whose unit changes have a decisive influence on the R_1 output. These are the following:

r_p – fire protection measures,
r_f – fire risk,
LPS – lightning protection level,

h_Z – type of special hazard,
L_0 – Internal System Failure (only hospital and explosion dangerous building in case of).

There are two parameters which raise the value of R_1 immediately above $1 \cdot 10^{-5}$, removing the lightning protection of the building. They are r_f and L_0. The other three parameters (r_p, h_Z and LPS) either raise R_1 immediately above $1 \cdot 10^{-5}$ or already touch the 25 % ($0{,}750 – 1{,}000 \cdot 10^{-5}$) security range. It is the task of the lightning protection designer to determine the amount of lightning protection that he/she is considering for certain buildings. Experience has shown that this ranges from 20 % to 25 %.

If the strong parameters are known, it can be a help the architect and the lightning protection designer. The design can be cheaper, simpler or faster. There is also an advantage of knowing the weak parts of the building: the "invisible" natural lightning rods of the building can be used during the design, in order to avoid any non-aesthetic elements on the building.

The sensitivity test results on several building types with 270 different attributes will be presented in the author's dissertation.

CONCLUSION

The calculations of the present study show that the examined 58 input parameters do not affect the output in the same way, so the new theses are the following:

- parameters can be grouped into strong and not strong parameters,
- in the strong parameters group, some parameters were identified as extremely strong (priority).

Based on the above, hypotheses 1 and 2 have been proved. The draft version of the standard has been rejected, and its content will be revised, so hypotheses 3 must also be rejected.

It must be emphasized that among these five parameters, two of them can be considered as extremely strong. It means that they always increased the risk value of the tested building by changing one unit immediately above the allowed R_T limit. These are the fire protection measures (r_f) and the failure of the building's internal systems (L_0)

In conclusion, the above calculations can help the architect and the lightning protection designer during the design period of the building. Knowing these parameters – weak points – of the buildings, the lightning protection design can be simpler, faster and in some cases, it can create a better-looking image. For example, it will allow the use of the natural elements of the building to avoid non-aesthetic lightning protection solutions which do not fit in their environment, and, as a result, the architect can keep the visual image of the building an that is important to maintain our cultural heritage for future.

REMARKS

[1]Strong parameter: parameters whose unit changes have a decisive influence on output.
[2]Extremely strong parameter: whose unit changes raises the output immediately above R_T allowed limit.
[3]OTSZ stands for Országos Tűzvédelmi Szabályzat, i.e. National Fire Protection Code.
[4]LPS stands for Lightning Protection Level.

REFERENCES

[1] Hungarian Standards Institution (MSZT): *MSZ EN 62305 series.*
Magyar Szabványügyi Testület Könyvtára, Budapest, 2011-2012,
[2] Kovács, K.: *Villámvédelem*.
Magyar Mérnöki Kamara, Elektrotechnikai Tagozat, Szakmai segédlet, Budapest, 2015,

[3] Bertus-Barcza, P.: *Lightning rod from one of the founding fathers.* https://ng.hu/kultura/2004/06/15/villamharito_az_egyik_alapito_atyatol, accessed 2nd September 2019,

[4] Kulcsár, L.: *Szigetelt villámvédelem (II.).* Elektroinstallateur **2**(5), 34-35, 2012, http://dx.doi.org/10.18773/austprescr.2012.015,

[5] –: *90% of the lightning strike damages was caused by secondary effects of lightning*. http://kamaraonline.hu/cikk/villamcsapas-a-karok-90-szazalekat-a-masodlagos-hatas-okozza, accessed 2nd June 2018,

[6] Novothny, F.: *Villamosenergia-ellátás II., 1. kötet Villamos biztonságtechnika*. Obuda University, Budapest, 2011,

[7] Hungarian Chamber of Engineers: *Risk analysis according to MSZ EN 62305-2.* https://docplayer.hu/4285330-Kockazatelemzes-az-msz-en-62305-2-alapjan.html, accessed 2nd February 2020,

[8] Hungarian Chamber of Engineers, Electrotechnical class: *National Fire Protection Regulations.* https://www.e-villamos.hu/cikkek/5358-letoltheto-a-legfrissebb-modositasokkal-szerkesztett-orszagos-tuzvedelmi-szabalyzat, accessed 17th February 2020.

Interdisciplinary Description of Complex Systems 18(3), 382-388, 2020

ARTIFICIAL INTELLIGENCE USAGE OPPORTUNITIES IN SMART CITY DATA MANAGEMENT

Luca F. Hudasi and László Ady*

NextTechnologies Ltd. Complex Systems Research Institute
Budapest, Hungary

DOI: 10.7906/indecs.18.3.8
Regular article

Received: 17 February 2020.
Accepted: 28 June 2020.

ABSTRACT

In our current study, we are aiming to explore data management methods in Smart City systems. In data management, Artificial Intelligence can be used as well. Solutions for the usage of Artificial Intelligence and integration into Smart City concept will be researched as well. Main motivation of the study is to draw attention to one of the most important element of Smart Cities, to the flow of data. Our study provides a possible solution for managing data and keep data up-to-date in such systems with the usage of newest technology possibilities. While explaining the solution, we will give all the necessary details about the data flow model between the Artificial Intelligence based system and humans who are using the Smart City. For managing the dataflow, we would like to use Big Data methods extended with other required methods. We are using the term of Big Data as a technology maximizing computation power and algorithmic accuracy to gather, analyse, link, and compare large data sets [1] connecting with Artificial Intelligence solutions.

KEY WORDS

smart city, artificial intelligence, data, management, innovation

CLASSIFICATION

ACM: 10010147.10010178
JEL: C8

*Corresponding author, η: adylaszlo@nexttechnologies.hu; -;
H- 2234 Maglód, Sugár út 44.

INTRODUCTION

Intelligent systems, such as Smart Cities are based on the flow of information [2]. Another important aspect of a good smart city is to make good decisions. It is logical, that if a system has bad or missing information, it cannot make good decisions [3].

'The first step in a city becoming a "smart city" is collecting more and better data.' [4] says John Walker in his study. Therefore the following main areas are important to cover upon collecting data:

Develop an automata data collector system.

Develop a people triggered data collector system.

Develop a data sharing and correction system.

The following figure shows the flow of data based on collection and sharing:

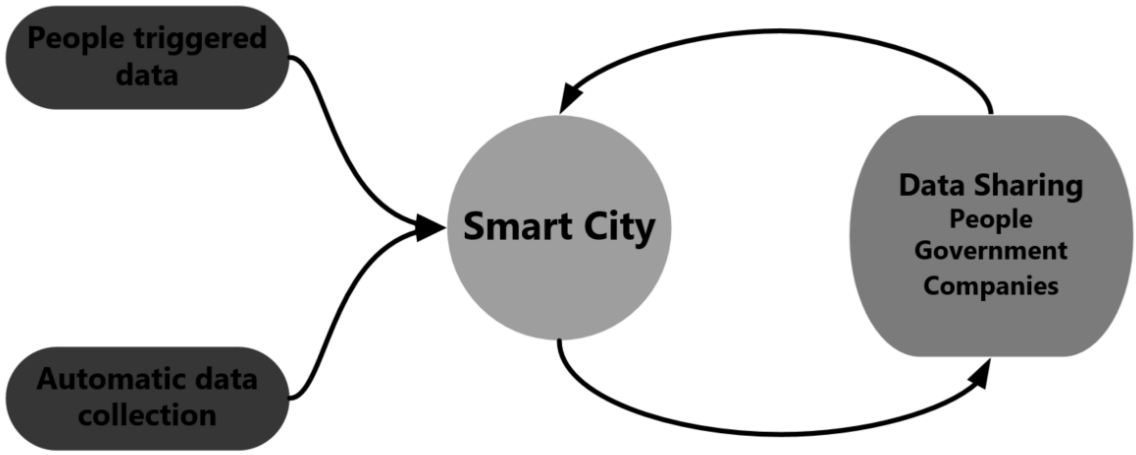

Figure 1. Data flow of a smart city.

On figure 1, arrows show the direction of data flow. Although people triggered data and Automatic data collection is mainly one directional, data sharing is not. Data Sharing part has many subcomponent and the data flow in this case bidirectional since the participants not just providing but getting data as well. In the following sections we discuss the details of each components.

DEVELOP AN AUTOMATA DATA COLLECTOR SYSTEM

Developing an automata data collector system covers the already well-known methods, such as having traffic monitoring systems, automata government administration bodies (for voting, for taxes, etc.), and an automata traffic-, weather forecast-, and energy distribution system. To build fully automated systems using big data, it is a requirement to have a built-out sensor network such as camera, temperature measurers, motion detectors and GPS based devices [5]. It does not mean these systems do not require a supervisor, but they can operate in an independent way and processing data coming from sensors. Many of these systems are already existing in testing or in live format, for example in Singapore, London, Barcelona, etc. [4, 6]. It is important to use the experiences from these cities to build a more reliable one.

DEVELOP A PEOPLE TRIGGERED DATA COLLECTOR SYSTEM

People triggered data collectors are Intelligent Systems where the information is coming from an active human input. Such as if an inhabitant visit an authorized system (through internet) and report or handle an administrative hace they need. For example request a credit, rent a

car, report a misdemeanour activity, etc. Here, the smart system has to be prepared to be able to serve the customer's need and make fair and clear decisions. This is the most dangerous form of Data Collection because the final decision is made by an Artificial Intelligence (AI) using a learnt scheme. The discrimination factor is too high, and there are already case studies for detecting and removing discriminative part from the software [7]. 'Some companies curtailed their customers' credit if charges appeared for counselling, because depression and marital strife were signs of potential job loss or expensive litigation' [8] says Racher O'Dwyer and this was just one example from the many. The question which should be considered is: is it ethical and legal to allow such kind of discrimination? If the answer is no, then the information system should be prepared to prevent this, or supervised for such actions. Connecting psychology and big data in the field of allowance is a new immature area which needs further studies and testing before essential decisions are made based on the result. Therefore, we strongly recommend to use a bipolar system in this case: first, the AI based system make the decisions using the source from collected Big Data, then a human supervisor should overview the output with the factors used in the decision, and validate or decline it. Using this 'two steps verification' looks longer, but it is not so much. Collecting data would be still the responsibility of the automata system and this is the most time-wasting part of the process. Educated human supervising would correct and develop the AI to make better decisions in the future. Once the system works measurably stable and ethical, the supervising work can be decreased.

Another important point of data collection is to collect quality data [4], otherwise the information the system's decisions are based on is corrupt or missing, therefore the decisions will be similarly wrong. To achieve this, our proposed solution is to include the inhabitants of the city to clarify data.

One area where inhabitants can participate is the social-, public administration improvements. The system would be capable of filling out data and do pre-tasks for the inhabitants (for example: doing the tax, requesting for new social cards when the existing ones are going out-of-date, providing public utility usages, making renting, other billing tasks, etc.) but the citizen would have the opportunity to monitor the decisions, and correct them if needed. Next time the system would learn from the mistakes and from the habits of the people, and would make better decisions.

Another are would be for extra comfort services, where people would voluntarily provide information for the system which then can help them to take away tasks from their shoulders, such as organizing trips, ordering and delivering food, other supplies, or appointments with doctors or similar. With more up-to-date corrections of the information and decisions the system is operating with are made, the better intelligent services could be provided. It is always very important to leave an opportunity to supervise the decisions the AI is doing in the place of people, to avoid discrimination and bad decisions (detailed above).

DEVELOP A DATA SHARING AND CORRECTION SYSTEM

To be able to cooperate with citizens in the development of data and decision-making, it is important to make the information – the smart city collects – as transparent as possible. People should see the base information of some bad decisions to be able to help to correct them.

While the smart city would provide transparent decision making for the citizens, it is critical to guard the sensitive data. Big data collection is always a hazard factor. More information the system provide, more value it represents and it will be more interesting for non-ethical parties. Therefore, any data which can be provided to third party, should be depersonalized carefully. To manage the proper depersonalization, is a key factor of the data flow. Creation of standards document for depersonalization of Smart City data is a requirement.

The main industry, which is collecting and using data is the advertisement industry. It can also produce a great income for the city by using the data collected, but the depersonalization should be act in the process here as well. People should been informed that the collected data are provided and generating income, but the system should also keep people's trust while do so. The first aim of a smart city is always to provide a better and easier life for people, get rid of discrimination and unethical decisions. Ethical and correct advertising is the part of this, but it should not lead to people exposed to direct marketing harassments which can lead to people leaving social media platforms and losing trust [9, 10].

There is another part of the industry, which is dealing with data: A company can provide other useful data for the smart city and in exchange get data as well which is important for the company. This can be a government level company as well which is collecting data and provide the result as a service for the people.

STRATEGY TO PROCESS DATA

After discussing the aspects of collecting and managing quality data, the next important step is to have the intelligent system make good decisions. We emphasized the need for supervising decisions till they become trustable in the aspects of avoiding discrimination and improvements. We offered the idea to include citizens in the supervising work as well. Also mentioned to use up data and experience collected from other smart cities. These ideas can help maintaining data decisions. Although we have to know that a good system beside having the correct data and algorithms also needs to process data quick and effectively. A good strategy to process data is taking the following steps: data filtering, pre-processing, processing and decision support. Figure 2 shows the processing stages with their dependencies.

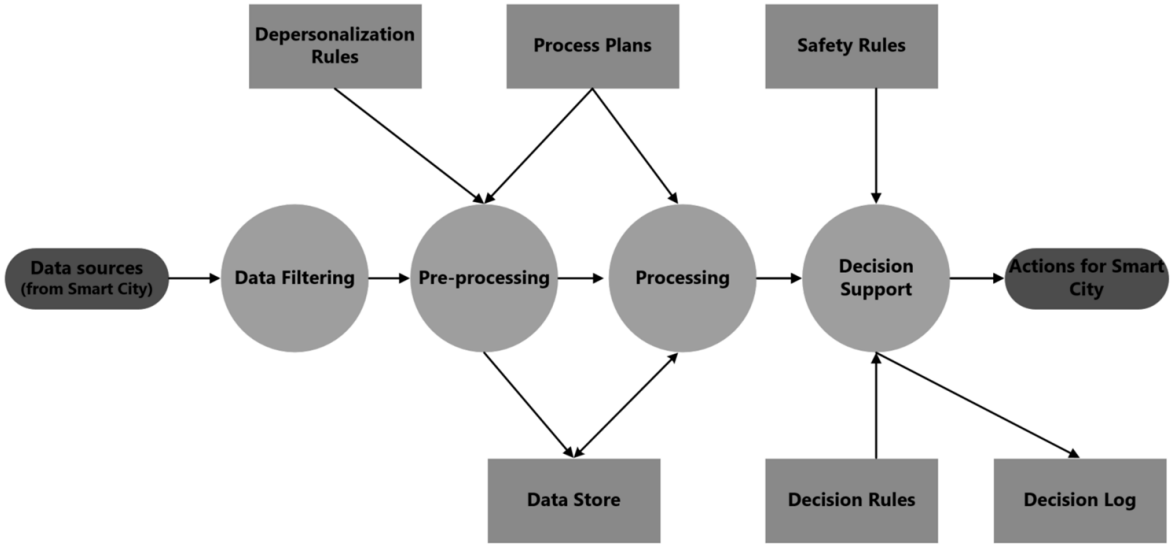

Figure 2. Logical architecture of data processing steps.

DATA FILTERING

The aim of data filtering is to collect data which the system really needs during the processing, to minimize the amount to store and process. An existing solution to filter out too many data (mainly when the system has limitations of processing quickly) is CERN's solution. CERN had a problem of bypassing all the measured data to their servers. With Intel's help, they developed a specific FPGA which help to filter out the relevant data before bypassing it to the servers. This way, they minimized the load on the centre [11].

PRE-PROCESSING

It is a good speeding strategy to execute pre-processing tasks as close at the point of data collection as possible. This means that the stage when the data comes in the system, stored procedures executed immediately and decode the input such as voice to text, picture to sort and identify, etc. Sorting (mainly of pictures) is an effective way because dedicated devices are already a stage of the sorting. As an example, a parking lot could have a dedicated camera to recognize empty spaces and another dedicated one for recognizing unauthorized parking. For pre-processing the pictures, the area reservation database needs to be presented at the moment the picture is catched and pre-processed by the camera system. This is the stage when the data depersonalization should be performed as well in case it is needed.

PROCESSING

Processing has many types how it can be performed. These types can be individually used or together as well. These types are the following:

1st type: Stored procedures. In this context, stored procedure means a logically separated unit of functions for performing a specific task. The sorting component will decide which stored procedure can be executed on the data by sorting it to categories. These procedures need to be written, but on the contrary it takes less processor time while they are running on production.

2nd type: AI. During the processing, an AI module will decide which AI based stored procedure can process the data,. These AI based stored procedures will only get pre-processed data. Raw data will be pre-processed by the sorting unit. These AI units (stored procedures) are looking for relations in data.

3rd type: Data mining. Using the opportunities of data mining, the system can learn models from big data to predict problems. After detecting upcoming problems, there is a possibility to make decisions to prevent them and create a safer environment. ‘Difficulties that need to be addressed during data mining include data gathering, data labelling, data and model integration, and model evaluation’ [12]. Data gathering and data labelling can happen in the pre-processing stage, data and model integration, and model evaluation should happen in the processing stage.

4th type: Manual. Manual actions needed In cases the system can not recognize and process a certain data from the pre-processing stage (because it is not prepared for it). The system will display the details on a graphical interface and will ask a human to decide the next steps, such as sorting the data into one of the existing categories. This type of processing is more like an extend method for “error handling” together with other AI based solutions.

DECISION SUPPORT

This stage of data processing is responsible to make automated decisions or help the human decision making.

Result after the processing stage is stored in a database. The decision supporting unit has the knowledge of the connections between result types and actions. Let’s take an example: There is a processing result that contains a picture that a car took a parking place. The connected action is to decrease the number of free spaces. The digital table in front of the parking lot will change and display the new data with the amount of free parking places. Or let’s take a more complex case example when the camera system detects that a big container occupied the public space near a building. The first action will be to check the permission of taking the place at the related authorities. In case there is no permission, the second action to execute is to create a draft report for the police (or related authority) and put the case up to a human supervisor to accept or decline. It is important to make this case half-automated with human

supervising, because making a punishment should not be full automated. The decision support unit has to contain a set of rules about which action can be done in which case: for example, at a heating system there could be a rule that after switching off the gas unit, it cannot be turned back in the next 5 minutes (safety period of the gas unit to chill down). If an automated decision would be made to turn on the heating because it is too cold within this 5 minutes, this rule would write it over. All the decisions which were made, should be logged for possible investigations and later improvements.

PROTECTION OF DATA FLOW

Finally, since smart cities are operating with sensitive data, it is also a part of data management to save the data from being stolen, unauthorised modifications and destruction. Beside using the well-known defensive solutions – since the system is based on artificial intelligence and there are couple of paradigms available of normal behaviours – we can use these resources to add another level of defence for the system's protection. We propose to build an alarm system, which – by monitoring the information flow – can alert about disharmonious data detections. Which means, if the data flowing through the system does not follow a continuously measured norm, it could be considered that the data was manipulated. This prevention method can be considered as a "software" type prevention. Physical prevention means that important data is allowed to travel on a way that is theoretically impossible to interfered or read by malicious bodies without immediate detection. In practise, this means the usage of optical cables where the network can detect any interference if the specifications of the light change. Using IEC 62443 standard is highly advised [13]. As a conclusion, we suggest to consider using the mentioned techniques and processes from this article when new smart cities are designed and build, and also for existing smart cities to develop.

REFERENCES

[1] Boyd, D. and Crawford, K.: *Critical questions for big data.*
Information, Communication and Society **15**(5), 662-679, 2012,
http://dx.doi.org/10.1080/1369118X.2012.678878,

[2] Tokody, D.; Papp, J.; Iantovics, L.B. and Flammini, F.: *Complex, Resilient and Smart Systems.*
In: Flammini F., eds: *Resilience of Cyber-Physical Systems. Advanced Sciences and Technologies for Security Applications.* Springer, Cham, 2019,

[3] Tokody, D.; Schuster, G. and Papp, J.: *Smart City, Smart Infrastructure, Smart Railway*.
International Conference on Applied Internet and Information Technologies, October 23, 2015.
Technical faculty "Mihajlo Pupin" Zrenjanin, Zrenjanin, 2015,

[4] Walker, J.: *Smart City Artificial Intelligence Applications and Trends.*
https://emerj.com/ai-sector-overviews/smart-city-artificial-intelligence-applications-trends, accessed 2nd February 2019,

[5] Neirotti, P.; De Marco, A.; Cagliano, A.C.; Mangano. G. and Scorrano, F.: *Current trends in Smart City initiatives: some stylised facts.*
Cities **38**(2014), 25-36, 2014,
http://dx.doi.org/10.1016/j.cities.2013.12.010,

[6] Ismail, N.: *What are the most advanced smart cities in the world?*
https://www.information-age.com/advanced-smart-cities-world-123470745/, accessed 2nd February 2019,

[7] Galhotra, S.; Brun, Y. and Meliou, A.: *Fairness Testing: Testing Software for Discrimination.*
ESEC/FSE'17, 4-8 September, 2017, ACM, Paderborn, 2017,

[8] O'Dwyer, R.: *Algorithms are making the same mistakes assessing credit scores that humans did a century ago.*
https://qz.com/1276781/algorithms-are-making-the-same-mistakes-assessing-credit-scores-that-humans-did-a-century-ago/, accessed 2nd February 2019,

[9] Morrison, K.: *Consumers Don't Like and Don't Trust Digital Advertising (Infographic).*
https://www.adweek.com/digital/consumers-dont-like-and-dont-trust-digital-advertising-infographic, accessed 3rd February 2019,

[10] Tenzer, A. and Chalmers H.: *When trust falls down.*
https://www.ipsos.com/sites/default/files/2017-06/Ipsos_Connect_When_Trust_Falls_Down.pdf, accessed 3rd February 2019,

[11] Barney, L.: *The FPGA based Trigger and Data Acquisition system for the CERN NA62 experiment*.
https://www.hpcwire.com/2017/04/14/xeon-fpga-processor-tested-at-cern, accessed 7th February 2019,

[12] Létourneau, S.; Famili, F. and Matwin, S.: *Data Mining to Predict Aircraft Component Replacement.*
IEEE Intelligent Systems **14**, 59-66, 1999,
http://dx.doi.org/10.1109/5254.809569,

[13] Elder, J.: *Understanding the Importance of Physical Security for Industrial Control Systems (ICS).*
https://applied-risk.com/blog/understanding-importance-physical-security-industrial-control-systems-ics, accessed 6th February 2019.

Interdisciplinary Description of Complex Systems 18(3), 389-399, 2020

AXIAL GAP OPTIMISATION OF HALF DIAMETER SHIFTED COUNTER ROTATING DUAL ROTOR WIND TURBINE

Csaba Hetyei[1,] * and Ferenc Szlivka[2]

[1]Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

[2]Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering
Budapest, Hungary

DOI: 10.7906/indecs.18.3.9
Regular article

Received: 11 March 2020.
Accepted: 28 June 2020.

ABSTRACT

General energy demand is continuously increasing due to the fact that wind turbines and other renewable energy sources have begun to appear in previously unexplored areas, such as on the roofs of buildings. In view of this demand, a new type of wind turbines described in this article could become one of the energy generating tools in a smart grid system. In this article, first conventional and unconventional wind turbines are reviewed with respect to efficiency. Then a Counter Rotating Dual Rotor Wind Turbine (CO-DRWT) construction is analysed with Computational Fluid Dynamics (CFD) codes considering a fixed radial and a variable axial distance. In the analysis, power coefficients were calculated for different configurations. It was found that in case of the dual rotor wind turbine, the optimal axial distance for half diameter radial shift was in the range of 0,2-0,25 diameter.

KEY WORDS

CFD, CO-DRWT, optimisation, smart grid, wind turbine for urban areas

CLASSIFICATION

ACM: I.6.2
JEL: O13, Q42
PACS: 47.11.+j, 88.50.G−

*Corresponding author, η: hetyei.csaba@phd.uni-obuda.hu; +36 1 666 5449;
Népszínház street 8., 1081 Budapest, Hungary

INTRODUCTION

Due to the increasing demand for energy, the extraction of renewable energy sources comes into focus increasingly frequently. Renewable energy has different sources depending on the potentials of the location.

By reviewing the global market of renewable energy sources, we can see a growing trend from year to year. By the study of Frankfurt School – UNEP Collaborating Centre for Climate & Sustainable Energy Finance [1] in 2018, the estimated new investment was 133,5 billion USD for solar, 129,7 billion USD for wind, 6,8 billion USD for waste energy technologies, such as biomass, 2 billion USD for geothermal, 481 million USD for biofuels, and 359 million USD for small hydro powers. The overall estimated new capacity installation cost was 272,9 billion USD, which is less by 12 % compared to the new investments in 2017. Researchers have been working on improving the power cycle efficiency in order to decrease the cost of renewable energy. For example, the use of supercritical CO2 as working fluid in power cycles has the potential to revolutionise power generation [2].

In the urban area where usually a traditional energy system is available, several base power plant provides the electricity. In contrast to the traditional system, in the smart grid next to the base power plant there are variable energy sources, i.e. renewable energy sources. The strength of this system is that any small scale energy sources could be the main power plant for a sub-system for a required time interval. For example, for small electrical devices like a coffee machine PV panels or small scale wind turbines could complete the available big scale power plant's electric production.

Focusing solely on the wind energy sector, the first wind turbine (WT) was invented by James Blyth in 1887, which was a vertical axis wind turbine (VAWT). The first horizontal axis wind turbine (HAWT) was invented by Charles Brush and built in 1888. This two WTs are shown in Figure 1.

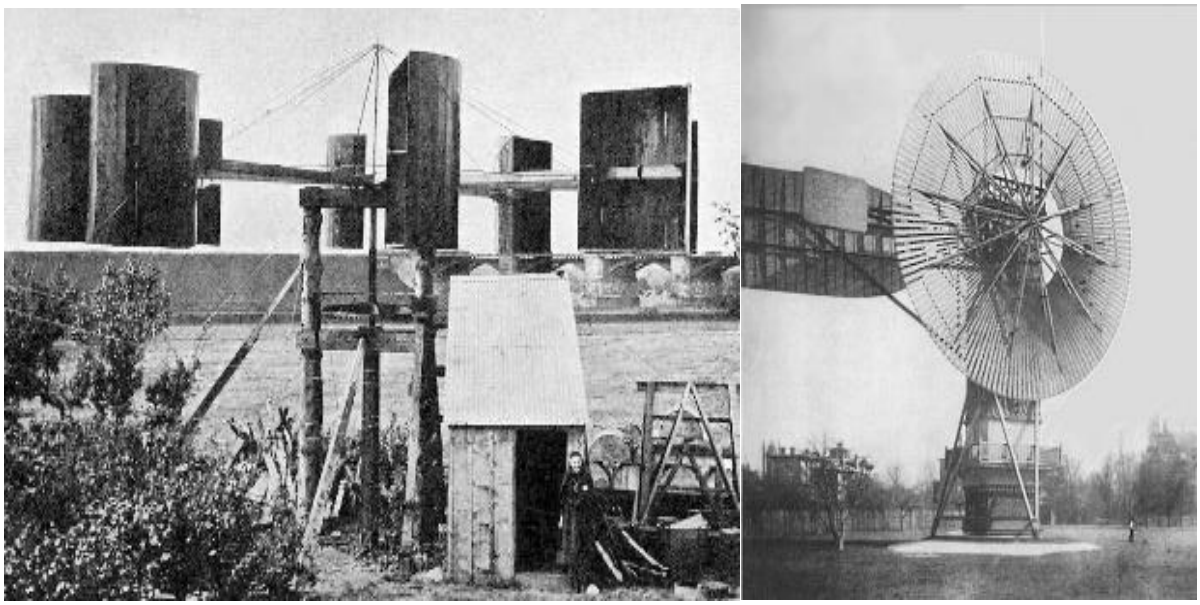

Figure 1. James Blyth's (left) and Charles F. Bush's (right) WT [3, 4].

While the first WT's structures were constructed of wood and canvas, nowadays turbines are constructed of steel, concrete, glass fiber and epoxy matrix composite materials. Thanks to these new materials and the growing demand for electricity, an increasing number of WTs appearing in the cityscape.

Figure 2. Wind turbines mounted on buildings. A) World Trade Center in Bahrain [5] b) Strata SE1 Tower [6].

Nowadays, due to the development and installation of a growing number of WTs, it is important to examine how multiple wind turbines in close proximity interact with each other and with the installation areas, such as buildings in the urban region. A. Nagy and I. Jahn [7]398 have shown a measurement system that is capable to measure flow parameters between wind turbines. The technology of WTs is evolving continuously to be more autonomous, sustainable and economical. Innovations helped in the development of new parts, e.g. guide baffles, new blade structures and profiles, some of which are shown in Figure 3.

Figure 3. Unconventional WTs. A) Guide baffle [8], b) Archimedes Screw Wind Turbine [9], c) Hi-Q wind turbine [10].

The layouts of multiple "standard" turbines used on the same tower may only be limited by imagination, as new structural innovations are being considered. There are different approaches when the turbines are installed on different axes or on the same rotating axis. For the latter type, depending on the rotating direction, the turbines are called co-rotating or counter-rotating dual rotor wind turbines (CR-DRWT and CO-DRWT). These unconventional WTs are shown in Figure 4.

Figure 4. Unconventional twin and multi WTs [11-13].

Lee et al. [14] simulated a CO-DRWT's power coefficient, c_p by using the blade element momentum theory and they compared it with a c_p of a traditional single-rotor wind turbine (SRWT). As a result, the CO-DRWT showed in some cases higher performance for different pitch angle, rotating speed and radius ratio compared to the SRWT.

The power coefficient, c_p, which we were refed can be calculated with the following equation:

$$c_p = \frac{P_{rotor}}{P_{wind}} = \frac{M \cdot \omega}{\frac{1}{2} \rho \cdot A \cdot v_\infty^3} \tag{1}$$

In the equation, P_{rotor} is rotor's power, P_{wind} is the wind power, M is the torque, ω is the angular velocity, ρ is the density of the air, A is the swept area, v_∞ is the freestream velocity.

Ozbay et al. [15] performed an experimental study to compare the power production performance of CR and CO DRWTs compared to SRWTs. They found the DRWTs' overall c_p was higher than the SRWT's. Furthermore, they found that the counter-rotating DRWT can harvest more energy than the co-rotating DRWT.

Theoretically, c_p has a maximum value, which was calculated as 16/27 (59,26 %) by the one-dimensional Betz's law, and 30,113 % by the two-dimensional GGS model [16]. By the measurement results for the SRWT, the maximum efficiency was shown to be in between the GGS and the Betz limit.

MOTIVATION

In this research, a CO-DRWT was studied without the tower and a nacelle. In our analyses, the propeller layout was chosen as being fixed as 0,5D radially, and with a variable axial distance between 0,005 and 2D. (The D in the distance values represent the rotor diameter, which was 200 mm.)

For the initial position, the 180° shifting between the mirrored wheels "top" planes were selected to avoid overlapping between the blades. The initial geometry and the labelled distances are shown in Figure 5.

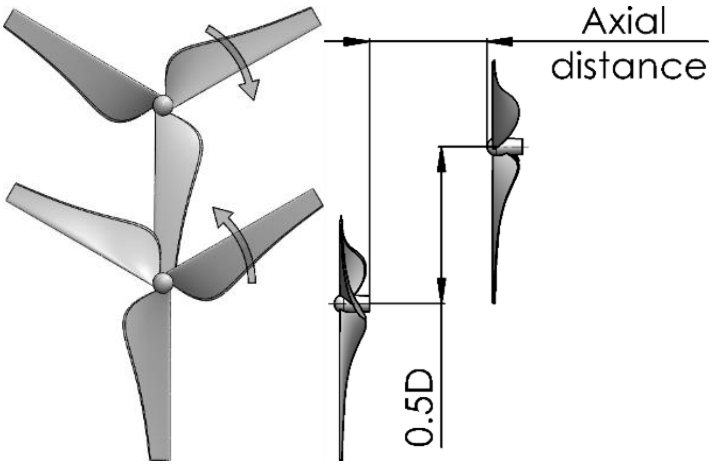

Figure 5. Studied counter-rotating dual rotor.

By numerical simulation, c_p values were calculated and compared for the studied cases.

SIMULATION AND EXPERIMENTAL METHODS AND SETTINGS

In the next subchapters, the finite volume method (FVM) is reviewed for the simulations, and our simulation's boundary conditions and measurement system are described.

SIMULATION METHOD

In the simulations, two different CFD (Computational Fluid Dynamics) software were used with the finite volume method.

The FVM divides the computational domain into finite volumes, and using the conservation laws (mass, momentum and energy) to compute the flow field properties. This calculation uses the transport equation of:

$$\frac{\partial}{\partial t}\int_V U\,dV = -\oint_A \underline{F}\,d\underline{A} + \int_V S_V\,dV + \oint_A \underline{S_A}\,d\underline{A} \tag{2}$$

In the equation, $\frac{\partial U}{\partial t}$ is the time-dependent member, U is a residual quantity's volumetric flux, F is the same residual's flux, S_V is the F flux's volumetric source, S_A is the F flux's surface source, V is the computational volume and A is the computational volume's surface.

The CFD codes solve this equation and its linked equations iteratively until the residual quantities do not decrease to a prescribed (near zero) value.

SIMULATION PARAMETERS

For the simulations, Mentor Graphics' FloEFD and Ansys CFX were employed.

In each simulation, we used air from the software's material database, which enters to the domain at the inlet face with 3,79 $m \cdot s^{-1}$ freestream velocity. The outlet faces had an environmental pressure of 1 atm, where the flow could quit from the domain. The wind turbine tip speed ratio was 4, which means the rotating region had 24,1279 RPS angular velocity.

For clarity, the tip speed ratio can be calculated by equation (3), where λ is the tip speed ratio, ω is the angular velocity, R is the blade's radius and v_∞ is the freestream velocity.

$$\lambda = \frac{\omega \cdot R}{v_\infty} \tag{3}$$

The simulation with FloEFD was in steady state with frozen rotor technique, and transient with the sliding mesh method. The unsteady simulation was run for 0,4144582 second, which is the time requirement for 10 rotations. In each state the k-ε turbulence model was used. In FloEFD, its own mesher was used, which provided a cartesian mesh with cell mating and cut-cell methods. For these simulations a rectangular computational domain was used (Figure 6).

For CFX, nearly the same boundary conditions were used as in FloEFD, with the following differences:

- for modelling the turbulence, the SST model was used,
- for meshing the body fitting and element sizing technique was used,
- a tubular computational domain was used (Figure 7).

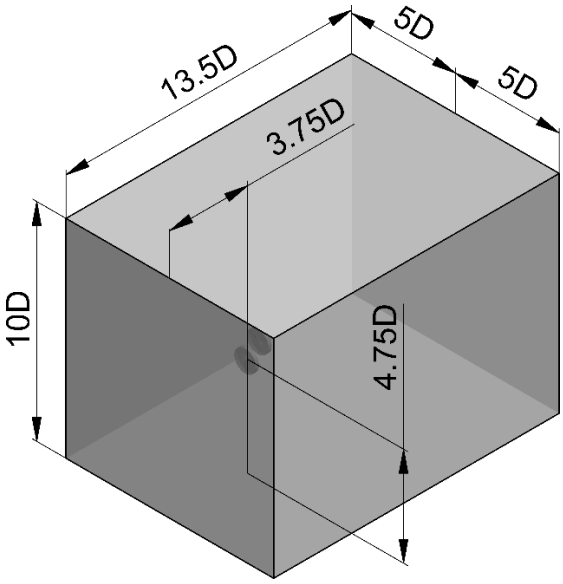

Figure 6. Computational domain for FloEFD.

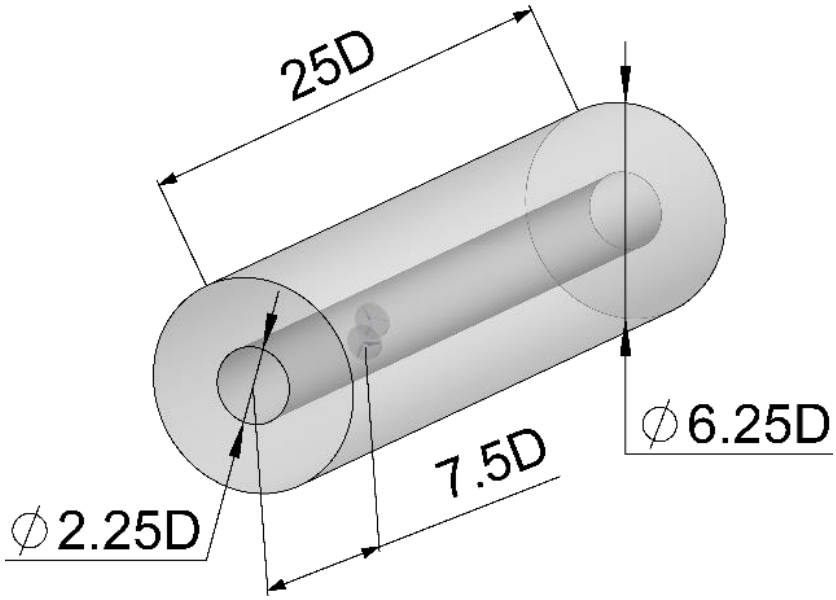

Figure 7. Computational domain for CFX.

Two different methods were used, the frozen rotor method (in steady state) for sweeping the whole axial range, and the sliding mesh technique (in unsteady state) for simulating the turbulence and checking the steady state result for the measured axial distance.

MEASUREMENT METHOD

For validating our simulation, a 3D printed version of the turbine wheels were used, which are shown in Figure 8.

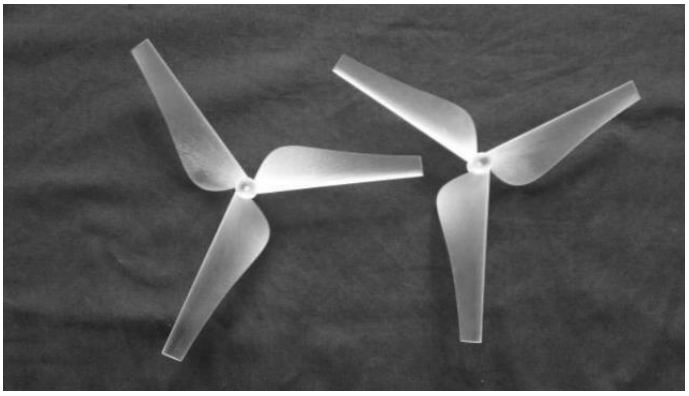

Figure 8. 3D printed wind turbine blades.

The printed wheels were taken into a wind tunnel (Figure 9) where we were able to measure the generated torque [17].

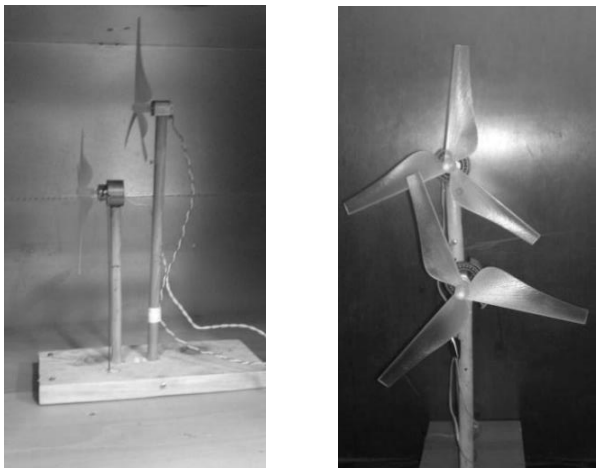

Figure 9. Wind turbines in the wind tunnel.

RESULTS

In the software for each axial distance the flow field was similar. In the next figure (Figure 10) the velocity distribution near the turbines for A = 0,5D distance is shown.

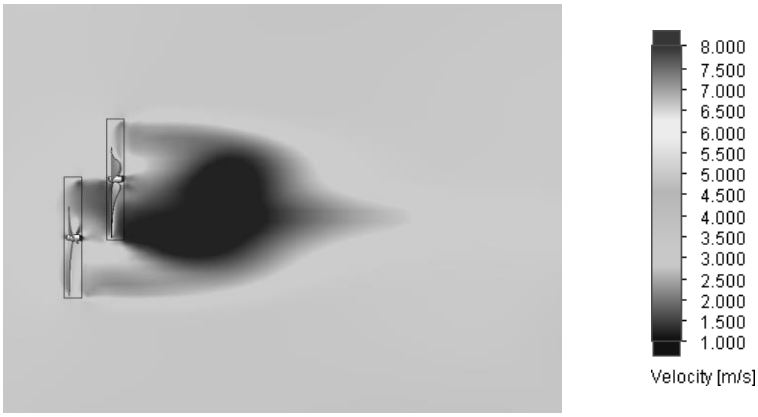

Figure 10. Velocity field for $A = 0{,}5D$ distance, in unsteady state (zoomed).

For comparing our simulations, we were monitoring the torque on the surface of the blades. At the end of the simulation, in steady state the simulation affords a single value for the torque, while in transient the CFD software a torque value was produced for each time step. These time series are shown in Figure .

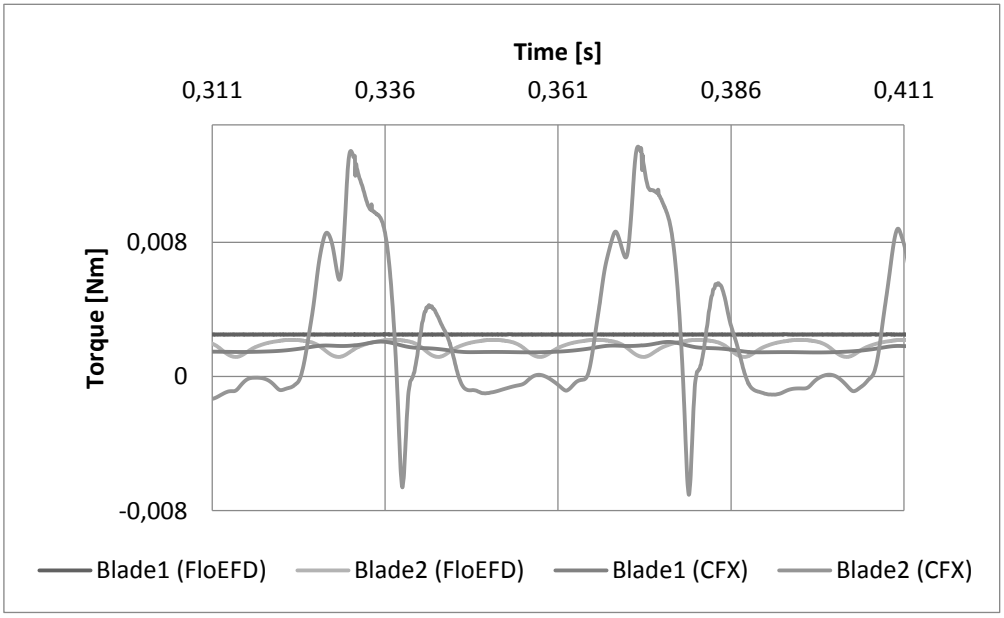

Figure 11. Torque values in the time domain.

The power coefficient (c_p) can be calculated from the torque and the boundary conditions. In Figure 12 the simulated c_p-s is shown, the frozen rotor technique (steady state) with blue dots, and the c_p with SST turbulent model in unsteady state (CFX) with the yellow square, and the c_p with k-ε turbulent model in unsteady state (FloEFD) with grey diamond, and the measured c_p with the red triangle. In each case, the c_p value is the sum of the two blades' power coefficients.

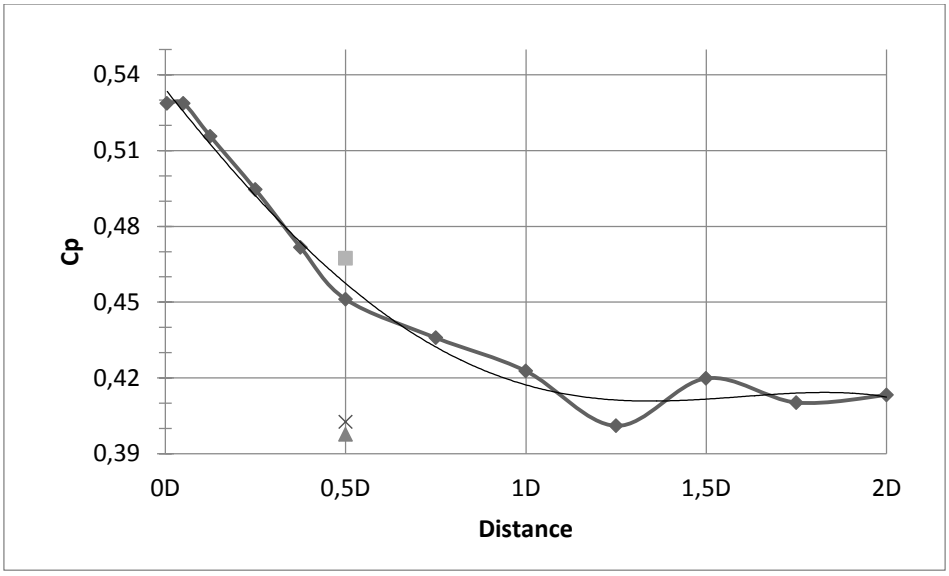

Figure 12. Power coefficient (c_p) versus the axial distance.

The simulated c_p with frozen rotor was 96,54 % while the simulated c_p with transient rotor stator was 86,15 % (with SST) and 86,08 % (with k-ε) of the measured c_p.

For comparison, we ran a simulation with frozen rotor technique for a one rotor turbine, and its power coefficient was 0,3424, which was 73,29 % of the measured CO-DRWT's c_p.

CONCLUSIONS

In this study, we were analysing a counter-rotating dual rotor wind turbine between 0,005D and 2D axial distance with a fixed 0,5D radial shift. At the end of the simulations, the power coefficient was plotted against the axial distance (Figure 11), and it was compared with a measured value.

Upon the results shown in Figure , the following statements can be established:

1) The power coefficient (c_p) was higher when the turbine wheels were closer.
2) In a built application, the zone before 0,2-0,25D was avoided, because the blade deformation could cause collisions.
3) The highest c_p was found at 0,05D. The second was at 0,005D, which is 0,01096 % smaller than value at A = 0,005D.
4) The dependence of the simulated c_p's with the distance can be modelled as $y = -0{,}0172 \cdot x^4 + 0{,}0487 \cdot x^3 + 0{,}0370 \cdot x^2 - 0{,}1792 \cdot x + 0{,}5343$ with the goodness of fit of $R^2 = 0{,}9874$.
5) The first wheel power coefficient (c_{p1}) and the second power coefficient (c_{p2}) were approximately the same in the 0,05-0,25D range.
6) After 1D axial distance, the c_{p1} value was 3 to 4 times larger than c_{p2}.
7) The SRWT's c_p value was 4,29 % larger than CO-DRWT's c_{p1} value for the 1.5D distance, 4,25 % more than the 1,75D's value and 3,01 % bigger than the 2D's value.

Upon conclusions 1) and 2), the recommended optimal distance was the closest where the blades do not have any collisions. For the required minimal distance, a measurement or a two-way FSI simulation is necessary.

We made the mesh dependency analysis for the A = 0,5D configuration, therefore, conclusion 3) might be a result of a numerical error. If not, the c_p of 0,05D has the largest value, therefore, it is energetically the best examined distance.

Regarding conclusion 7), we can establish that for large axial distance (like the 1,5-2D), a counter-rotating DRWT first rotor produces similar power like a single SRWT, therefore, the second rotor produces the extra power.

Based on the conclusions of the presented study, the CO-DRWT has a large potential as an engineering application for increased wind energy harvesting at small places where it is needed, such as in the urban areas of smart cities.

REFERENCES

[1] Frankfurt School-UNEP Centre: *Global Trends in Renewable Energy Investment 2019.* https://wedocs.unep.org/bitstream/handle/20.500.11822/29752/GTR2019.pdf, accessed 20th September 2019,

[2] Braden, T., et al.: *The University of Queensland Refrigerant and Supercritical CO2 Test Loop.* ASME Turbo Expo 2016: Turbomachinery Technical Conference and Exposition, Seoul, 2016, http://dx.doi.org/10.1115/GT2016-58110,

[3] –: *James Blyth's Wind Turbine*. https://upload.wikimedia.org/wikipedia/commons/1/13/James_Blyth%27s_1891_windmill.jpg, accessed 23rd September 2019,

[4] –: *Charles F. Brush Wind Turbine*. https://media2.fdncms.com/clevescene/imager/tilting-at-windmills/u/zoom/2622441/cover-3.jpg, accessed 23rd September 2019,

[5] –: *World Trade Center in Bahrain.* http://www.alternative-energy-news.info/images/pictures/wind-powered-towers.jpg, accessed 1st January 2019,

[6] –:*Strata SE1 Tower.* https://upload.wikimedia.org/wikipedia/commons/d/d8/Strata_SE1_from_Monument_2014.jpg, accessed 1st January 2019,

[7] Nagy, A. and Jahn, I.: *Advanced Data Acquisition System for Wind Energy Applications.* Periodica Polytechnica Transportation Engineering **47**(2), 124-130, 2019, http://dx.doi.org/10.3311/PPtr.11515,

[8] –:*Unconventional Wind Turbines.* http://www.whirlopedia.com/images/wind-turbines-elk.jpg, accessed 8th October 2019,

[9] –: *Bizarre Wind Turbines.* https://cdn.trendhunterstatic.com/thumbs/urban-wind-turbine.jpeg, accessed 8th October 2019,

[10] –: *Hi Q Wind Turbine.* https://www.darcorp.com/wp-content/uploads/2018/09/hi-q-wind-turbine-featuredLG.jpg, accessed 8th October 2019,

[11] Romańsk, L. et al.: *Estimation of operational parameters of the counter-rotating wind turbine with artificial neural networks*. Archives of Civil and Mechanical Engineering **17**(4), 1019-1028, 2017, http://dx.doi.org/10.1016/j.acme.2017.04.010,

[12] –: *Vestas Wind Turbine Tree.* https://landartgenerator.org/blagi/wp-content/uploads/2016/04/191838856_b2b14fff9e_o.jpg, accessed 8th October 2019,

[13] Laan, M.P. et al.: *Power curve and wake analyses of the Vestas multi-rotor demonstrator.* Wind Energy Science **4**(2), 251-271, 2019, http://dx.doi.org/10.5194/wes-4-251-2019,

[14] Lee, S.; Kim, H.; Son, E. and Lee, S.: *Effects of design parameters on aerodynamic.* Renewable Energy **42**, 140-144, 2012, http://dx.doi.org/10.1016/j.renene.2011.08.046,

[15] Ozbay, A.; Tian, W. and Hu, H.: *Experimental Investigation on the Wake Characteristics and Aeromechanics of Dual-Rotor Wind Turbines.*
Journal of Engineering for Gas Turbines and Power **138**(4), 1-15, 2016,
http://dx.doi.org/10.1115/1.4031476,

[16] Gorban, A.N.; Gorlov, A.M. and Silantyev, V.M.: *Limits of the Turbine Efficiency for Free Fluid Flow.*
Journal of Energy Resources Technology, **123**(4), 311-317, 2001,
http://dx.doi.org/10.1115/1.1414137,

[17] Szlivka, F.; Molnár, I.; Kajtár, P. and Telekes, G.: *CFX Simulations by Twin Wind Turbine.*
2011 International Conference on Electrical and Control Engineering. IEEE, Yichang, 2011,
http://dx.doi.org/10.1109/ICECENG.2011.6057550.

Interdisciplinary Description of Complex Systems 18(3), 400-407, 2020

THE HUNGARIAN NUCLEAR EMERGENCY RESPONSE SYSTEM

Hullán Szabolcs*

Hungarian Atomic Energy Authority
Budapest, Hungary

DOI: 10.7906/indecs.18.3.10
Regular article

Received: 23 March 2020.
Accepted: 5 August 2020.

ABSTRACT

The Hungarian Atomic Energy Authority embodies the guarantee of the peaceful and safe use of atomic energy for the Hungarian society (and indirectly for the citizens of neighbouring countries). It is the responsibility of the Hungarian Atomic Energy Authority to guarantee safety complying with international standards and recommendations, and adhering to and complying with national standards. The Hungarian Atomic Energy Authority is also responsible for coordinating the national nuclear emergency response system and helping in decision making.

KEY WORDS

International Atomic Energy Agency, international and national cooperation, nuclear emergency response, nuclear safety of cities

CLASSIFICATION

JEL: E65
PACS: 21.00.00

*Corresponding author, η: szabolcs.hullan@gmail.com; +36 20 915 5724;
H-1173 Budapest, Új street 5, Hungary

INTRODUCTION

The International Atomic Energy Agency (IAEA) provides for the application of standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities (with nuclear and radiological emergency preparedness), as well as it serves as an intermediary among its Member States for this purpose. Designated authorities, or organizations responsible for the management of emergencies recognize that good preparedness in advance of any emergency can substantially improve the emergency response [1]. It is an international expectation that IAEA member states (and its authorities) meet this IAEA general requirement. This is especially important after the Fukushima Dai-ici accident.

In Hungary the Hungarian Atomic Energy Authority (HAEA) embodies the guarantee of the peaceful and safe use of atomic energy for the Hungarian society (and indirectly for the citizens of neighbouring countries). It is the responsibility of the HAEA to guarantee safety complying with international standards and recommendations, adhering to and complying with national standards. The HAEA is independent from all organizations involved in the development and technical support of nuclear energy, which is a fundamental requirement for national and international organizations. Figure 1 shows how Hungarian issues of complex international effects.

The responsibility of the authority is to supervise safety and protected applications, to prepare regulations in accordance with the results of science and technology, to make the licensee observe the requirements of the law, to ensure the conditions provided by the Hungarian Parliament and Government, and to establish and operate a competent and effective regulatory body within the legal framework. Security, safety and safeguards can have several meanings in the energy sector. Security of the energy supply; protection or security (physical protection) and peaceful uses (i.e. the user is not building nuclear weapons) are various aspects of security. Safeguards are measures that guarantee the peaceful use of nuclear energy and prevent the proliferation of nuclear weapons. Nuclear protection (physical protection) security means protection against deliberate human action. The protection against the harmful effects of the ionizing radiation is called nuclear safety – the protection of the environment, as well as people (both the general public and employees) and all living things from the harmful effects of ionizing radiation.

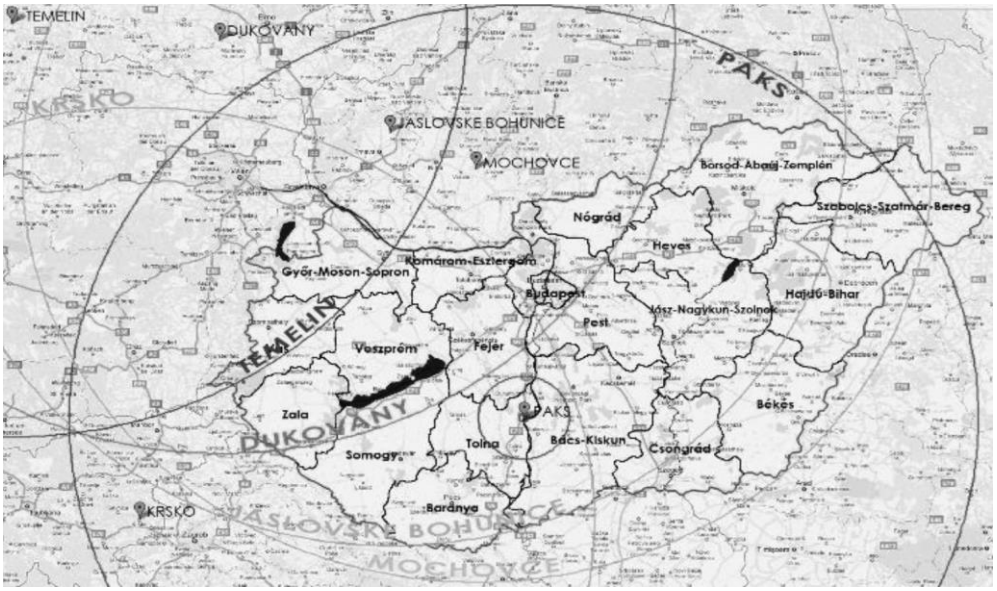

Figure 1. The nuclear threat of Hungarian cities from various nuclear power plants [2].

Emergency response is an important task of the HAEA, which is independent from nuclear facilities, but integrates all the regulatory fields. Operating an Emergency Response Organization within the HAEA which is internationally acknowledged and meets the IAEA standards and requirements was a major challenge.

TASK OF THE AUTHORITY

REQUIREMENTS

The HAEA is a supervisory body in the field of accident management programmes and emergency response systems of nuclear facilities. The IAEA Safety Guides [3, 4] provides recommendations for the development and implementation of an accident management programme to meet the requirements for accident management that are established in the publications.

Accident management, including severe accident management, is therefore an essential component of the application of defence in depth. Accident management complements the operating procedures that must be developed for normal operation, anticipated operational occurrences and accident conditions, as stated in the IAEA Guide [4]. The operating organization of the power plant shall establish, periodically review and as necessary revise the accident management program. The accident management program has to integrate accident management guides, too. The accident management guidance should be an integral part of the overall emergency arrangements and should be coordinated with the on-site emergency plan, established in accordance with the IAEA publication [4, 5], as well as the national legislation and authority requirements.

OFFICIAL DUTIES

The main tasks of the HAEA are licensing, assessment, inspection and enforcement. Licensing is one of the most responsible areas for the authority's activity. The license is always based on a safety analysis to demonstrate the guarantee of nuclear safety, while relevant regulatory requirements and special requirements [5] are taken into account. The emergency response and action plans, as well as the accident management guides of nuclear facilities are licensed by the HAEA.

Inspection takes places during the realization of the activity; it reveals the facts and circumstances of the activities and it gives opportunity for intervention in the implementation phase. The Authority is involved in all nuclear emergency response exercises and drills. Sometimes this participation is only an administrative role, but in case of the annual comprehensive drills the HAEA ERO is activated as well.

The authority performs the assessment typically during an activity or a process, so the conclusions are drawn subsequent to the completion of the activity.

Licensing, inspection and assessment are not fully separate activities: they may and frequently must supplement each other for the appropriate oversight of a certain case.

Enforcement means imposing fines or withdrawal of license, and this is the ultimate possibility to enforce the legal requirements and regulatory point of view.

The task of the Authority is to take part in the nuclear emergency response and preparedness system and to operate an Emergency Response Organization. According to the Atomic Act [6] and the relevant Governmental Decree [7] several tasks belong to the HAEA in the field of nuclear emergency preparedness and response.

THE IMPLEMENTATION OF PREPAREDNESS IN HAEA

THE HUNGARIAN NUCLEAR EMERGENCY RESPONSE AND PREPAREDNESS SYSTEM (NERS)

The national nuclear emergency response system takes care of preparations to respond to radiological and nuclear events occurring in the course of the peaceful use of atomic energy. The NERS is responsible for the mitigation and reduction of the consequences of any incidents.

The NERS operates in normal or, in some cases, in higher operational states, which can be readiness, alert, emergency and recovery operation. The normal state ensures the preparation for incidents. The readiness operation state is the sum of radiation protection activities applied in incidents that do not exceed the emergency threshold. It covers incidents that occur in a foreign country (in a nearby nuclear facility) and cause a radioactive release, or the risk of release is high, or an exposure occurred in Hungary, but the emergency threshold is not exceeded, although the risk of radioactive release is high. The operational state can be changed from the normal state, for example, if an incident occurs in a facility that uses radioactive materials, such as exposure in a hospital. In the emergency operations state, protective actions must be introduced in order to decrease the resident population's exposure or risk of exposure to radiation [8-10].

The NERS is the totality of central, ministerial, territorial and local level organizations and bodies concerned in the prevention, mitigation of consequences and elimination of event causing unplanned radiation exposure to the public.

The governmental coordination body tasked with disaster management-related decision support to the government directs the NERS. The operational state of the NERS can be changed by the Minister of Interior, who is responsible for disaster management. The head of the HAEA can initiate this change with the head of the professional disaster management organization.

The NERS is responsible for supporting the decision making of the governmental coordination body in the field of protective actions as well.

MINISTRIES PARTICIPATING IN THE NERS

Ministry of the Interior, Ministry of Human Capacities, Ministry of Defence, Ministry of Foreign Affairs, Ministry of National Economy, Ministry of National Development, Ministry of Rural Development are represented at the ministerial level in the NERS. The Minister of the Interior is the chair of the Coordination of Disaster Management.

INDEPENDENT ADMINISTRATIVE BODIES AND MINISTRY DEPARTMENTS

The following independent regulatory organizations, national law enforcement organizations and ministry departments also participate in the NERS: the Hungarian Atomic Energy Authority, the National Directorate General for Disaster Management, the National Food Chain Safety Office, the National Office of the Chief Medical Officer, the Hungarian Defence Forces, the Hungarian Police Headquarters, the National Tax and Customs Office, the General Directorate of Water Management, and Pest County Government Office (as national environmental protection authority).

REGIONAL AND LOCAL PARTICIPATION

Local defence committees coordinate the response at the regional level and inform the public in the region. Town mayors coordinate the response within their jurisdictions, and other local organizations supports the NERS decision making.

In accordance with the recommendations of the IAEA, Hungary issued the National Emergency Response Plan in 2002. In 2017 the third edition was issued. The goal of the National Nuclear Emergency Response Plan is to summarize all those requirements and tasks that have importance in achieving basic goals in off-site response to a nuclear emergency due to the use of atomic energy affecting the territory of Hungary. The Hungarian NERP provides a framework and guidance to prepare the central, departmental, regional, local and facility emergency response plans and preparedness. The HAEA ERO (see next section) is involved in the NERP approval sequence.

OPERATION OF THE HAEA EMERGENCY RESPONSE ORGANIZATION

The HAEA operates an Emergency Response Organization (ERO) that maintains close liaison with the NERS (see the organizational diagram, Figure 2.) The ERO is a contact point both to international organizations and to nuclear facilities. It is also a competent authority, based on Hungary's EU membership and the international conventions on early notification and assistance in the case of nuclear emergency. The ERO is responsible for the assessment of nuclear and radiological conditions during an emergency. [8-10]

HAEA experts operate the Centre for Emergency Response, Training and Analysis (CERTA), and this is the operational location for the ERO. It is designed for monitoring and analysing the nuclear and radiological emergency and for supporting the decision making process by making simulations and nuclear / radiological assessment.

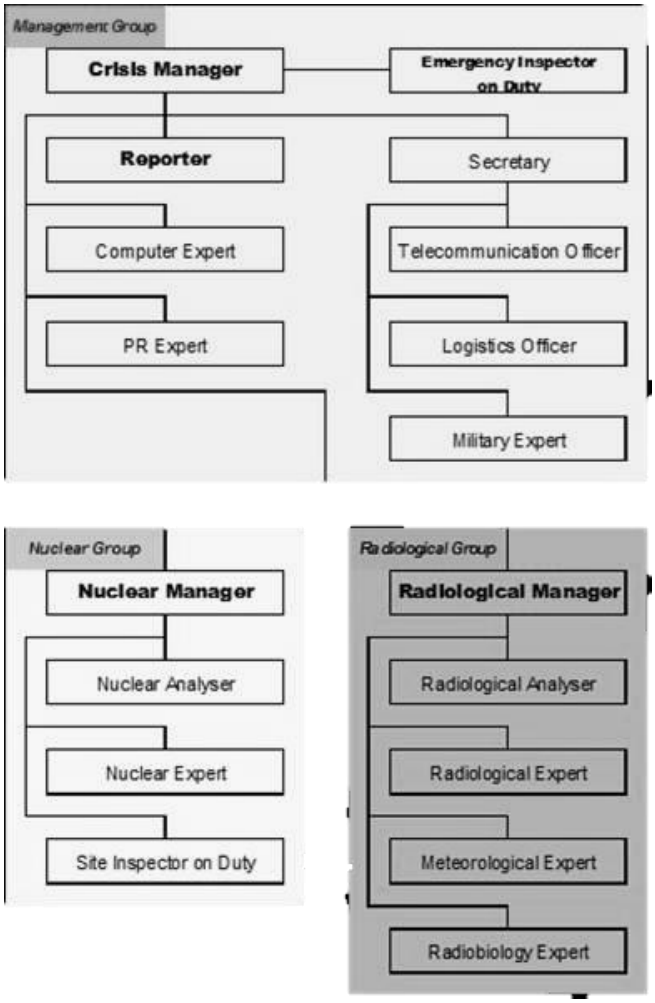

Figure 2. The structure of the ERO operated by HAEA.

ERO's Nuclear group is responsible for nuclear analyses, the Radiological group is responsible for radiological analyses and the national radiological monitoring systems, while the Management group is responsible for the coordination and the approval of the subordinated groups' reports. The Crisis Manager, as the final approval authority, is responsible for all documents formulated and dispatched by the ERO.

The Emergency Officer on Duty is the contact point with external organizations, and he supports the work of the ERO. The Site Inspector on Duty delegated to the emergency organization of the Hungarian Electricity Works (Magyar Villamos Művek – MVM) at the nuclear power plant in Paks collects the on-site information.

One of the tasks of the HAEA Nuclear Safety Inspector on Duty is to receive the nuclear and radiological event notifications from locations within Hungary. He is on standby around the clock to receive fax or phone notifications. The notifications of nuclear emergencies from abroad, on the other hand, are received by the Emergency Inspector on Duty. The two duty officers are equipped with smart phones, via which they can send and receive fax and email messages and initiate phone calls. The Nuclear Safety Officer on Duty records the incoming reports and takes appropriate actions under his own authority in case of less significant incidents (which occur more frequently), while in an emergency he informs the Crisis Manager on Duty.

Subsequent to the decision on alerting of the HAEA ERO due to an exercise or real emergency, the notification goes through the organization according to the pre-established alert-chain.

INTERNATIONAL COOPERATION

The purpose of the international co-operation is to improve the efficiency of regulatory instruments and the effectiveness of the activity by exchanging experiences and understanding international conventions, codes, safety requirements, recommendations, guides, training courses and international good practice. Each Member States of the IAEA is responsible for conducting a periodic review of its emergency preparedness and response capabilities. The IAEA has guidelines for states and international organizations to develop arrangements to interface with the IAEA and with the other member states in case of a nuclear or radiological incident or emergency [11]. The IAEA has interagency framework for preparedness for and coordinated response to nuclear or radiological incidents and emergencies [12]. This Joint Radiation Emergency Management Plan (JPLAN) defines the co-operation among organizations on an international level (European Commission, Police of the European Union – EUROPOL, Food and Agriculture Organization – FAO, IAEA, International Civil Aviation Organization – ICAO, INTERPOL, International Maritime Organization – IMO, OECD Nuclear Energy Agency – OECD-NEA, Office for the Coordination of Humanitarians Affairs – OCHA, United Nations Scientific Committee on the Effects of Atomic Radiation – UNSCEAR, World Health Organization – WHO and Wold Meteorological Organization – WMO). The IAEA has a task to coordinate the response to nuclear or radiological emergencies, the OCHA coordinates humanitarian response, the WHO and PAHO coordinates public health response and IAEA member states responsible for the international assistance and release of public information. The structure of the JPLAN is shown in Figure 3.

The IAEA has a coordinator role, in case of a nuclear and radiological emergency on an international level.

The IAEA triggers the activation of the system, receives notifications of emergency, acts as the focal organization for response coordination, and coordinates international assistance.

Hungary is a member of the IAEA operated Response Assistance Network (RANET). The

HAEA has a role as a national coordinator among the Hungarian assistance organizations. In 2011 RANET has 19 countries with registered capabilities.

The legal framework of international cooperation in the field of nuclear emergency response is provided by the conventions on early notification [11] and mutual assistance in case of a nuclear or radiological emergency, which were established under the auspices of the International Atomic Energy Agency and the Euratom directive on the community regulations concerning early information exchange in radiological emergencies. According to the international requirements for the receipt of early notifications and the dispatch of such notification in a timely manner in case of domestic emergencies, the HAEA operates its competent authority duty system on a 0-24 basis. There is international cooperation on nuclear emergency management. Based on this convention the IAEA's Unified System for Information Exchange in Incidents and Emergencies (USIE) system is used for early notification, and the RANET system is used for mutual assistance in the case of nuclear or radiological emergency.

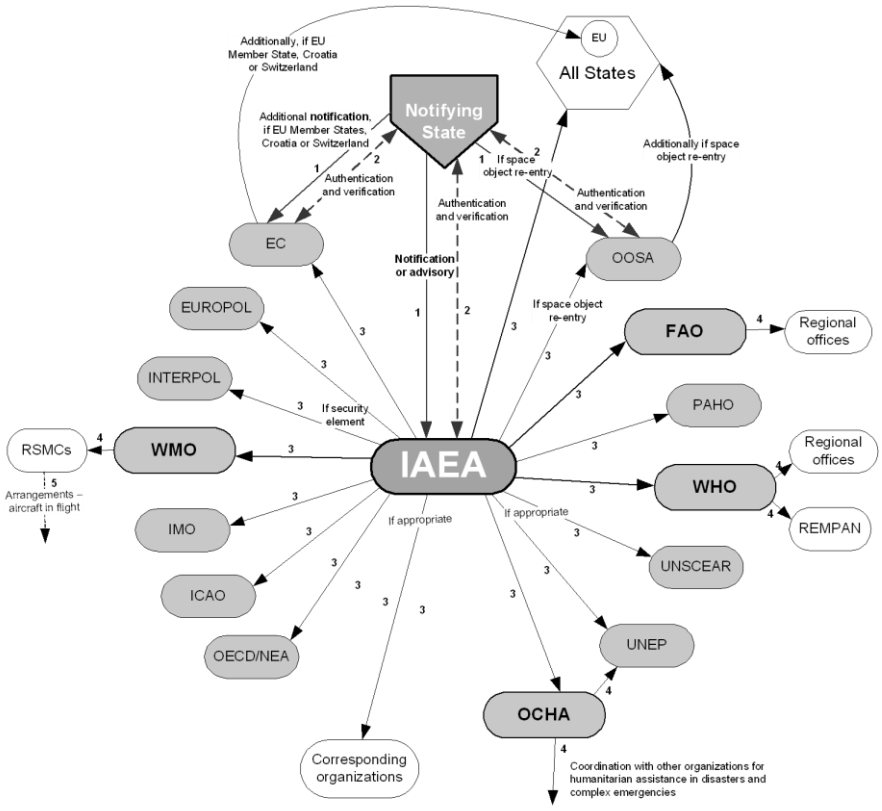

Figure 3. The structure of the Joint Radiation Emergency Management [12].

Hungary concluded bilateral agreements with Austria, the Czech Republic, Croatia, Germany, Romania, Slovakia, Slovenia, Ukraine and Serbia to notify each other of nuclear or radiological emergencies in the early phase of such situations and assist each other should such a request be received. The bilateral cooperation agreements provide good opportunities to share experiences, organize joint exercises and elaborate the framework of joint activities.

CONCLUSION

In the framework of RESPEC (Radiological Emergency Support Project for the European Commission) the HAEA has become a supporting organization, delegating experts who analyse radiological events in the radiation protection section in radiological or nuclear emergency situations. The HAEA ERO has won RESPEC tenders three times to perform

support tasks. The HAEA was activated and supported the European Commission successfully during the Fukushima Daiichi Accident in 2011.

REFERENCES

[1] IAEA: *General Safety Requirements – Preparedness and Response for a Nuclear od Radiological Emergency.*
GSR Part 7 (2015),

[2] Kátai-Urbán, L. and Kiss, B.: *Nukleáris erőművek, mint veszélyes technológia és az országos nukleárisbalesetelhárítási rendszer.*
Hadmérnök **9**(3), 80-97, 2014,

[3] IAEA: *Specific Safety Guide - Accident Management Programs for Nuclear Power Plans.*
SSG-54, 2019,

[4] IAEA: *Method for Developing Arrangements for Response to a Nuclear or Radiological Emergency.*
EPR-METHOD, 2003,

[5] IAEA: *Method for the Development of Emergency Response Preparedness for Nuclear or Radiological Accidents.*
IAEA-TECDOC-953, International Atomic Energy Agency, Vienna, 1997,

[6] IAEA: *General Safety Requirements – Safety of Nuclear Power Plants: Commissioning and Operation.*
SSR 2/2, 2016,

[7] –: *Act CXVI of 1996 on Atomic Energy*.

[8] –: *Govt. Decree 167/2010. (V.11.) on national nuclear emergency preparedness and response*.

[9] –: *Govt. Decree 487/2015. (XII.31.) on ionization radiation*.

[10] –: *Govt. Decree 489/2015. (XII.31) on the monitoring of the environmental radiation situation and levels of radioactivity in Hungary*.

[11] –: *Joint Radiation Emergency Management Plan of International Organization*.
EPR-JPLAN, 2010,

[12] –: *Convention on Early Notification of a Nuclear Accident and Convention on Assistance in the case of a Nuclear Accident or Radiological Emergency*.
IAEA, 1986.

MANUSCRIPT PREPARATION GUIDELINES

Manuscript sent should contain these elements in the following order: title, name(s) and surname(s) of author(s), affiliation(s), summary, key words, classification, manuscript text, references. Sections acknowledgments and remarks are optional. If present, position them right before the references.

ABSTRACT Concisely and clearly written, approx. 250 words.

KEY WORDS Not more than 5 key words, as accurate and precise as possible.

CLASSIFICATION Suggest at least one classification using documented schemes, e.g., ACM, APA, JEL, PACS.

TEXT Write using UK spelling of English. Preferred file format is Microsoft Word. Provide manuscripts in grey tone. For online version, manuscripts with coloured textual and graphic material are admissible. Consult editors for details.

Use Arial font for titles: 14pt bold capital letters for titles of sections, 12pt bold capitals for titles of subsections and 12pt bold letters for those of sub-subsections. Include 12pt space before these titles.

Include figures and tables in the preferred position in text. Alternatively, put them in different locations, but state where a particular figure or table should be included. Enumerate them separately using Arabic numerals, strictly following the order they are introduced in the text. Reference figures and tables completely, e.g., "as is shown in Figure 1, *y* depends on x …", or in shortened form using parentheses, e.g., "the *y* dependence on *x* shows (Fig. 1) that…", or "… shows (Figs. 1-3) that …".

Enumerate formulas consecutively using Arabic numerals. In text, refer to a formula by noting its number in parentheses, e.g. expression (1). Use regular font to write names of functions, particular symbols and indices (i.e. sin and not *sin*, differential as d not as *d*, imaginary unit as i and not as *i*, base of natural logarithms as e and not as *e*, x_{n} and not x_n). Use italics for symbols introduced, e.g. $f(x)$. Use brackets and parentheses, e.g. {[( )]}. Use bold letters for vectors and matrices. Put 3pt of space above and below the formulas.

Symbols, abbreviations and other notation that requires explanation should be described in the text, close to the place of first use. Avoid separate lists for that purpose.

Denote footnotes in the text by using Arabic numerals as superscripts. Provide their description in separate section after the concluding section.

References are listed at the end of the article in order of appearance in the text, in formats described below. Data for printed and electronic references is required. Quote references using brackets, e.g. [1], and include multiple references in a single bracket, e.g. [1-3], or [1, 3]. If a part of the reference is used, separate it with semi-colon, e.g. [3; p.4], [3; pp.4-8], [3; p.4, 5; Ch.3]. Mention all authors if there are not more than five of them, starting with surname, and followed with initial(s), as shown below. In other cases mention only the first author and refer to others using et al. If there are two or more authors, separate the last one with the word "and"; for other separations use semicolon. Indicate the titles of all articles, books and other material in italics. Indicate if language is not English. For other data use 11pt font. If both printed version and the Internet source exist, mention them in separate lines. For printed journal articles include journal title, volume, issue (in parentheses), starting and ending page, and year of publication. For other materials include all data enabling one to locate the source. Use the following forms:

[1] Surname, Initial1.Initial2.; Surname, Initial1.Initial2. and Surname, Initial1.Initial2.: *Article title.*
Journal name **Vol**(issue), from-to, year,
http://www.address, accessed date,

[2] Surname, Initial1.Initial2. and Surname, Initial1.Initial2.: *Book title*.
Publisher, city, year,

[3] Surname, Initial1.Initial2.; Surname, Initial1.Initial2., eds.: *Title*.
In: editor(s) listed similarly as authors, ed(s).: *Proceedings title*. Publisher, city, year.

If possible, utilise the template available from the INDECS web page.

CORRESPONDENCE Write the corresponding author's **e**-mail address, **t**elephone and **a**ddress (i.e., η).

ISSN 1334-4684 (printed)
http://indecs.eu