17(1-A), pp.1-84, 2019 **ISSN 1334-4684**

INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS

Scientific Journal

Scientific Journal
INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS

INDECS, volume 17, issue 1, part A, pages 1-84, year 2019
Published 29th March 2019 in Zagreb, Croatia
Released online 31st March 2019

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)

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 weak before the publishing date.

TABLE OF CONTENTS

EDITORIAL: KEY FACTORS FOR CREATING SMART, SUSTAINABLE AND RESILIENT CITIES

The present thematic issue of INDECS examines the driving forces behind smart and resilient city implementations. The philosophy behind the design of smart cities is to respond to the people's needs rather than trying to impose new developments on them. Local communities must be involved in the work of creating successful smart cities, for example, in the form of crowdsourcing, because by taking part in the development process, they will adopt these changes more easily. During this process, the public's needs must be constantly analyzed, which must be followed by the retesting of suggestions and solutions of the experts and citizens involved, in an iterative way. The essence of the pioneer "smart" concept is the development of a common, synergic cooperation of different urban structures with the purpose of creating more livable cities.

In order to create such inclusive, safe, resilient and sustainable cities, certain indicators must be defined with regard to the provision of various services and the quality of life. Besides the results of international and European best practice efforts, the importance of a holistic approach to cities and the issues of cities as complex systems must also be considered.

It is equally important to draw attention to the relationship between various research topics (e.g. smart technologies, autonomous cars, drones, data mining, etc.) and the emerging sustainable safe city implementations. The urban structures and technological advances presented in this thematic issue mark the arrival of sustainable development in local communities, where these intelligent and smart systems will cover all aspects of life.

Therefore, the primary aim of the present thematic issue is to offer researchers an opportunity to extend their existing scientific knowledge in the field of emerging key technologies, including, among others, the use of drones, cybersecurity methods, blast protection, smart materials, soft computing methods, autonomous vehicles, Critical Infrastructure Protection, safe city technologies, energy efficient buildings, 5G mobile networks, intelligent transport systems, water management, emergency management, business continuity and community resilience. All of these in the service of a single purpose: to create safe, sustainable and resilient cities and communities which can successfully face the challenges of the future.

Cordially,

Budapest, 25th February 2019

Guest editors:

Prof. Dr. Sci. Gyula Mester

Dipl.-Ing. Dániel Tokody

Interdisciplinary Description of Complex Systems 17(1-A), 1-6, 2019

A THREAT FOR THE TRAINS: RANSOMWARE AS A NEW RISK

Daniel Vaczi and Tamas Szadeczky*

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

DOI: 10.7906/indecs.17.1.1
Preliminary report

Received: 11 October 2018.
Accepted: 31 December 2018.

ABSTRACT

Nowadays we cannot speak about cybersecurity as a simple problem. It is not just about users cannot properly use the devices because of a malware settle in their computers.

Now professionals have to work in a more complex system. The information technology meshes most of our life. Begin with people use their smartphones over that companies lead most of their processes via computers.

Nations want that their citizens can live in a healthier, more comfortable, economical place, so they started to think about how can they warrant a better life. Result in this governments started to make critical infrastructure more economical with the help of information technology. That is how Smart Cities began to evolve. However, bringing into practice these innovations is still not enough. If we use any technology, we shall use it securely, that is why we must build our advanced city as a secure Smart City. If not, our systems can be attacked in different ways.

In the view of last years, we can accept, that ransomware can make considerable problems in different systems. Last time NotPetya caused many problems in Ukraine's infrastructure. The metro and the airport information technology systems were also victims of this malicious code. The security of the transportation is essential not just because of public transport one of the leading part of Smart Cities, but because in these public vehicles many people travel day by day, so these are critical infrastructures.

This article is processing what could happen if Hungarian train management systems got attacked by ransomware. What are the risks and how should we protect against them?

KEYWORDS

malware, ransomware, transport management systems

CLASSIFICATION

ACM: K.6.5.2
JEL: R41

*Corresponding author, η: szadeczky.tamas@kvk.uni-obuda.hu; +36 1 666 5170;
1084 Budapest, Tavaszmezo u. 17., Hungary

INTRODUCTION

As computers adhere to our life, we should prepare for new threats. Besides that information technologies help us to live our life easier, faster and more comfortable we can also run into trouble because of them. If we are looking around in the place where we are right now, there is an excellent chance that we can find many electrical devices. As time is moving forward, those objects become smarter and smarter. In this case, it just means that our articles of personal use are connected to the internet and may be integrated with a processor what helps to the electrical stuff serve our growing latent needs. Not just our homes and offices are going to be smarter with the help of the Internet of Things (IoT) devices, but also our cities. The concept of Smart Cities is more known and popular day by day. It means that we would like to turn our Planet and our environment more livable. For example, we would like to use the energy sources efficiently and also we would like to optimise our transport no matter if it is personal or public. Nowadays we can hear a lot about smart cars using artificial intelligence, which is one of the new and future ways of transporting. On the other hand many urban development programs purpose the expansion of public transport with the help of networking, analysis and machine learning. As we can see, those developments are heading to computers more heavily.

Unfortunately, this modern, information technology (IT) centralised word has a dark side also. In the last years, we can see new attacking trend in the cyberspace [1]. It has many dimensions. Cyberwars, an attack against companies or persons. On the one hand, we can found offensive where the attacker does not care who will be the victim; the only goal is the successfulness. On the other hand, there is a pre-elected person, group or company. The motivation of the attacker also can be different for example information and money gathering, ransom, gaining access to systems, destroying infrastructures, political or military motivation, and influencing.

ABOUT THE RESEARCH

Nowadays ransomware is one of those threats what makes the IT security professionals annoyed. This malware can block a company's life if the security system is unwell designed. The problem in a standard IT system is easily visible. Ransomware encrypts the whole disk with the data of the company, or it makes the device unreachable locks the input tools are locked. The higher problem when in a not protected critical infrastructure is under attack. The public transportation's IT systems are like that. Weakly protected, but if a planned attack can be successful, it can cause serious injuries or even death.

The authors researched the threat of ransomware in the available scientific articles, including categorisations, main scientific issues and protection possibilities. The focus of the research was the applicability of general ransomware issues to railway traffic control systems, to determine its susceptibility. The article is a preliminary research article about ongoing research shown in the acknowledgements.

RANSOMWARE AS A THREAT

The attackers have many opportunities to achieve their goal. They can use many tools on the different platforms depending on what is their motivation. In recent years, so-called ransomware attacks got attention. If ransomware successfully infects a device the content of it will not be available. Depending on the type of malware, it can just lock the screen and in the same time prohibit the access or encrypt the important files of the user or the Master Boot Record (MBR), perhaps other file indexes.

If we see the lifecycle of a typical ransomware attack, the first step is the distribution with the help of e-mail attachments, website compromises or similar [2; p.152]. Then the malware infects the victim system and starts to communicate with the encryption-key servers. After the connection is made, it searches for the commonly used file types, and it is typically renaming, encrypting and renaming them again. If the victim is on the company network, the backup methodology will be attacked, too [2; p.151]. At the end of the process the user will see a ransom message what says if the user pays, usually, in Bitcoin or other cryptocurrencies, the attacker will provide the decryption key.

Maybe those are not the most sophisticated attacks, but they are effective. Because of such an attack the user is going to realise the importance of information security while losing personal data. If the family photos become encrypted and finally lost, that is something what everybody can realise. But not just the private sector can be a victim of ransomware. The public organisations and the governmental sector also can be attacked by ransomware. In this case, we can easily concede that critical infrastructures (e.g., transport, banking, energy, health sector) and critical information infrastructure (e.g., telecommunication, internet access, satellites) are an excellent goal to the criminals or maybe other malicious nations [3].

There were two huge global ransomware attacks in 2017. One of it is called WannaCry (also known as WanaCrypt0r or WannaCrypt) [4]. Among other things the British health sector had a severe breakdown because of that malware campaign. The other globally concerned one from 2017 is the NotPetya (in other names: Petya, Petrwrap, ExtPetr). It is mostly attacked targets in Ukraine, but it also impaired one of the biggest container ship companies, the Danish A.P. Moller – Maersk Group. As a result of the campaign the shipping company still has unknown containers. Metro and Airport IT system were also targets of this attack. As we can see in these examples, critical infrastructures are deeply concerned with this problem.

Because writing a ransomware code is one of the most straightforward malware programming tasks, attackers use it frequently. We also have to remark, that nowadays anybody can buy ransomware as a service. It has a name, called RaaS (Ransomware-as-a-Service) [2; p.145].

TYPES OF RANSOMWARE

Al-rimy et al. defined a ransomware taxonomy in their paper, shown in Figure 1 [2]. They distinguished consumer and organisation target based attacks. They also separated this malware what is the attacked platform (e.g., PC, mobile, cloud). In our view, the most essential taxonomy is the severity based one. We can distinguish between those that are detrimental and what is only called scareware. The latter is just a fake warning. With the help of this trick, the attacker asks for a ransom without real damage. That ransomware what cause damage can be categorised as locker and crypto. If the malware only locks the services and limit the applications, we call it locker-ransomware. If it encrypts the user's files named crypto-ransomware. Depending on the cypher algorithm it can be classified as symmetric crypto-ransomware (SCR), asymmetric crypto-ransomware (ACR) and hybrid key crypto-ransomware (HCR). The SCR operates mostly DES, AES and RC4, the ARC use such as RSA and HCR integrate both previous algorithms.

PROTECTION AGAINST RANSOMWARE

As we could see via WannaCry and NotPetya, well-written ransomware can cause huge trouble. In extreme cases, it threats also life. In the IT security profession, most of the people agree that the security awareness is crucial [5]. The users are not careful, do not think on security in typical situations and because of those, the attacker can trick them easily. Maybe we think that in critical infrastructure the co-workers are more aware, but they can also be spoofed [6].

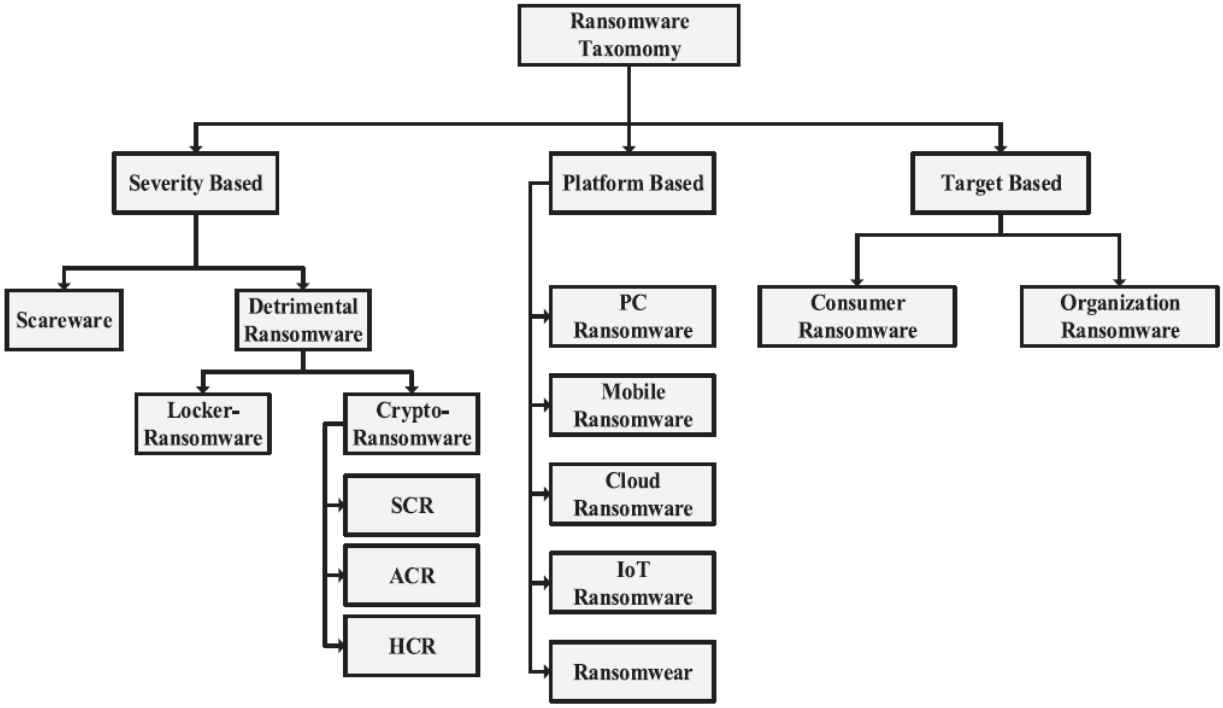


Figure 1. Taxonomy of ransomware [2].

The first step against any cyber-attack is to raise awareness and education level. Of course, this is not the only way to protect ourselves and our IT systems in the cyberspace. There is a need for technical countermeasures also, like system hardening and virus protection.

If a user opens an infected email attachment or surf a hacked webpage, a ransomware dropper can be downloaded. Those are the most common way to be attacked. However, if our IT system and processes are well prepared the malware has less chance to work. Steven Furnell and David Emm in their study introduce the three most crucial steps of defence against these malicious codes [4]. "A" as Anti-malware, "B" as Back-up and "C" as critical patching. Building an alarm system what gives us a signal if something strange or dangerous came into our system is necessary, even if it is not 100 % trustworthy. Then if we have a proper offline backup process in our system, we are able to recover the stored data. Finally, if we update the operating system, firmware and all possible software the ransomware cannot exploit the known vulnerabilities.

On the one hand those steps are too general, but if we look deep into the problem, those are necessary but not sufficient. Against the ransomware, the employees should notice if they are under attack and they have to know the needed steps to minimalise the loss. Knowing about the infected links and attachments is not equal to staying clear of them. Another easy but effective action is the unplugging of the computer. It can save many essential files.

SUSCEPTIBILITY OF RAILWAY TRAFFIC CONTROL

Transportation is always a crucial element of critical infrastructure. Sometimes people can forget how important the railway transportation is. It is not only about personal travel, but also a significant percent of cargo is transported by trains. As we can see, this kind of transportation is significantly vulnerable to the information technology aspect. There are many railway-related services what are now IT based. Timetable, geolocation, and surveillance of the trains are based on traditional IT-infrastructure. Typically this means a centralised IT service is running on a small number of servers. In this case, not just backups,

but also high redundancy is required, which is a question of investment. If the geolocation-based controlling system became hamstring, it might have a severe impact on the train control. In this way, the standard traffic management process will not work. The fallback solution is the manual control of the switches, stations and trains, which have a low throughput. Safety systems are based more on specialised hardware. However, similarly to industrial control systems, if we connect them to the internet, they will be susceptible to hacker attacks [7]. If the security modules of the modern railway control systems are exploited with ransomware, many people's lives will be jeopardised. The ticketing systems typically include web interfaces. Thus web services and web applications might be hacked. If ransomware infects a ticketing system front- or backend, the online and ticket office sales and also the ticket control might have stopped. Thus not just the buying, but also the travel is jeopardised. Those things can cause a shortage of the income and the dissatisfaction of the travellers. Interconnection interfaces between international train management systems are also implemented via the internet.

Even in the traffic control systems virtualisation and sometimes private clouds take place. From the CIA-triad (Confidentiality, Integrity and Availability) of information security, integrity deals with protection against malicious or unintentional modification of data stored in storages and sent through communication channels. According to standard information security, practice redundancy and error checking are the most common measures of integrity controls. In virtual data storages also concurrent and collaborative access issues became important. Availability is the ability to access data whenever required. Redundant data storage and processing, backup and business continuity management are the standard controls for that. Virtual systems are scalable, intelligent, flexible and redundant when they are built according to general best practice. However, the hypervisor is a new single point of failure because it is generally not redundant. Despite generally proper security controls, virtualised systems are not invulnerable. Amazon EC2 Easter outage in 2011 April was an example of cloud failures when more thousands of websites were unreachable because of a configuration error, which was possibly a human error. According to a study, the human factor is always an issue in information security. Therefore awareness should be increased [8, 9].

CONCLUSIONS

One can see that ransomware can cause massive damages. Maybe the impact is only a financial loss, but it can also risk human life. The only way to defend that system is proactivity.

In the case of railway companies, many different systems are being used. Also, some of them are non-conventional PC systems, but industrial IT elements. IT management should deal with the patching of those systems, despite the heterogeneous environment. Using anti-malware and universal threat management (UTM) is a matter of course. Last but not least we must raise the security awareness of the employees to avoid spreading the ransomware on the network with clicking on some malicious attachments.

ACKNOWLEDGMENTS

This article is based on the research conducted within the project "The Development of Integrated Intelligent Railway Information and Safety System", Application number: GINOP--2.2.1-15-2017-00098.

REFERENCES

[1] Yaqoob, I. et al.: *The rise of ransomware and emerging security challenges in the Internet of Things.*
Computer Networks **129**(2), 444-458, 2017,
http://dx.doi.org/10.1016/j.comnet.2017.09.003,

[2] Al-rimy, B.A.S.; Maarof, M.A. and Shaid, S.Z.M.: *Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions*.
Computers & Security **74**, 144-166, 2018,
http://dx.doi.org/10.1016/j.cose.2018.01.001,

[3] Rajnai, Z. and Puskas B.: *Requirements of the installation of the critical informational infrastructure and its management*.
Interdisciplinary Description of Complex Systems **13**(1), 48-56, 2015,
http://dx.doi.org/10.7906/indecs.13.1.7,

[4] Furnell, S. and Emm, D.: *The ABC of ransomware protection.*
Computer Fraud & Security **2017**(10), 5-11, 2017,
http://dx.doi.org/10.1016/S1361-3723(17)30089-1,

[5] Szadeczky, T.: *Information Security Law and Strategy in Hungary*.
Academic and Applied Research in Military and Public Management Science **14**(4), 281-289, 2015,

[6] Kiss, D. and Váczi D.: *Risks of attacks against human networks of companies and critical infrastructures according to network sciences*.
Hadtudomány **28**(1), 151-168, 2018,
http://dx.doi.org/10.17047/HADTUD.2018.28.1.151,

[7] Zimba, A.; Wang, Z. and Chen, H.: *Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems*.
ICT Express **4**(1), 14-18, 2018,
http://dx.doi.org/10.1016/j.icte.2017.12.007,

[8] Metalidou, E. et al.: *The Human Factor of Information Security: Unintentional Damage Perspective.*
Procedia – Social and Behavioral Sciences **147**, 424-428, 2014,
http://dx.doi.org/10.1016/j.sbspro.2014.07.133,

[9] Iantovics, L.B. et al.: *Review of Recent Trends in Measuring the Computing Systems Intelligence.*
Broad Research in Artificial Intelligence and Neuroscience **9**(2), 77-94, 2018,

Interdisciplinary Description of Complex Systems 17(1-A), 7-12, 2019

APPLYING RISK MANAGEMENT PROCESS IN CRITICAL INFRASTRUCTURE PROTECTION

Maria Luskova* and Zdenek Dvorak

University of Zlin, Faculty of Security Engineering
Zlin, Slovakia

DOI: 10.7906/indecs.17.1.2
Regular article

Received: 18 June 2018.
Accepted: 31 December 2018.

ABSTRACT

Critical Infrastructure is an asset or system whose disruption or destruction should have adverse effect on the performance of economic and social functions of the state, and thus on the quality of life of residents in terms of the protection of their life, health, security, property, as well as the environment. Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of all developed countries. The Slovak Republic has already adopted some legal standards and measures emphasizing the importance of critical infrastructure issues and aiming at ensuring the required level of its security and protection.

The article deals with the tasks and competences of state administration authorities in the area of critical infrastructure and the obligations of the operators in the protection of the critical infrastructure element in the Slovak Republic. It provides also a framework, application of risk management process as a foundational concept for processing security plan, designed to protect the element of critical infrastructure from disruption and destruction. In conclusion it emphasizes the need of close cooperation between public and private sectors to ensure proactive approach to securing critical infrastructure.

KEYWORDS

critical infrastructure, security, resilience, security plan, risk management

CLASSIFICATION

JEL: H12, H84, J28

*Corresponding author, η: maria.luskova@fbi.uniza.sk, +421 41 513 6766;
Univerzitna 8215/1, 010 26 Žilina, Slovakia

INTRODUCTION

Over the last twenty years technologically developed countries give increased attention to the question of the critical infrastructures protection (CIP). New threats, the dynamical development of technologies, continuous changes in the politics and economics increase the need to search for more effective ways to protect people, property and environment, situated in the certain area.

European Council Directive 2008/114/EC [1] defines a concept of the European Critical Infrastructures (ECI), which became the basis for the way of identifying the most important elements of national infrastructure in the different countries of the European Union. For simplicity, it is possible to state that the ECI is s a set of the most important elements of the national critical infrastructures each of the concerned countries.

The critical infrastructure (CI) is the part of national infrastructure; i.e. selected information systems, services, organizations, and their important objects and facilities; whose destruction or disruption, as a consequence of its exposure to certain risk factor, will cause a danger or disturbance in the society functioning or threat to life and health of the citizens. In fact, the particular system or service will be considered as a potential CI element if it will fulfill the significant role for some sector which can significantly affect security.

CIP is very actual topic. The involved countries had progressively established a legal framework of CIP on the national base (e.g. in Slovakia it is Act No. 45/2011 Coll. on Critical Infrastructure, in the Czech Republic it is the Act No. 240/200 Coll. on Crisis Management, in Poland it is document The National Critical Infrastructure Protection Programme). It can be stated that critical infrastructure is in developed economics part of the security system of the state.

For a correct understanding of CI it was necessary to define list of critical infrastructure sectors. In the most countries involved in the European Programme for Critical Infrastructure Protection (EPCIP), the major European sectors of CI are:

- energy (electricity, gas, oil industry, mining),
- information and communication technologies (satellite communication, networks, data centers, sources of classified information, control and information systems of infrastructures, etc.),
- transport (road, rail, air and water).

added with other areas important to the society functioning, such as the provision of drinking water, food security, financial sector, infrastructure of medical equipments and others.

CRITICAL INFRASTRUCTURE IN SLOVAKIA

The Slovak Republic (SR) as a member of the European Union participates in development of documents concerning the CI and especially their incorporation into legislative framework. At present, the issues of CI in the SR are codified in the act No. 45/2011 Coll. of 8 February 2011 on Critical Infrastructure (hereinafter Act) [2]. The Act provides the organization and competence of state administration authorities in the area of CI, the procedure for designating elements of CI and the obligations of the operator in the protection of the CI element and liability for breach of these obligations. CI includes a defensive infrastructure under a special regulation. Administration in the field of CI is performed by the Government of the SR, Ministry of the Interior of the SR and Ministries indicated in Table 1. Their competences as well as the obligations of the CI operators are defined by the Act. In the SR the CI sectors under the competences of central authorities are defined in Table 1.

Table 1. Critical Infrastructure Sectors under the competence of central authorities [2].

Sector	Sub-sector	Central authority
1. Transport	Road transport Aviation transport Water transport Railway transport	Ministry of Transport, Construction and Regional Development of the Slovak Republic
2. Power industry	Mining Electrical Energy Gas industry Oil and oil products	Ministry of Transport, Construction and Regional Development of the Slovak Republic
3. Information and communication technologies	Internet Information systems and networks	Ministry of Economy of the Slovak Republic
4. Electronic communications	Satellite communication Networks and services of stable and mobile electronic communications	Ministry of Finance of the Slovak Republic
5. Post	Providing postal services, post system of payments and administering activities	Ministry of Transport, Construction and Regional Development of the Slovak Republic
6. Industry	Pharmaceutical industry Metallurgical industry Chemical industry	Ministry of Economy of the Slovak Republic
7. Water and atmosphere	Providing drinking water Water buildings Meteorological service	Ministry of the Environment of the Slovak Republic
8. Health Services	N.A.	Ministry of Health of the Slovak Republic

Important documents except of the current version of Act No. 45/2011 Coll. on CI, related to the protection of critical infrastructure in Slovakia are, in particular, the National Program for Protection and Defense of CI in the SR, the Concept of Critical Infrastructure in the SR and related Act No. 319/2002 Coll. on Defense of the SR, Act No. 261/2002 Coll. on Prevention of Serious Industrial Accidents, the National Action Plan for Combating Terrorism, Act No. 129/2002 Coll. on Integrated Rescue System, Act No. 387/2002 Coll. on Management of State in Crisis Situations Other Than Time of War and State of War, and other [3].

OBLIGATIONS OF OPERATORS

The responsibility for protecting and defending critical infrastructure in the SR holds the public administration together with the owners and operators of the CI elements.

An important part of the law is the formulation of basic duties of operators of CI elements. Operators are required to take all necessary measures to protect the CI element and thereby ensure its functionality, continuity and integrity of the element's activities in order to prevent, avert or mitigate threats of disruption or destruction.

Significant aspects in relation to the operator's obligations include:

- developing and updating the operator's security plan,
- practicing a model situation of a threat of disruption or destruction of the element according to the security plan at least once every three years,
- designating an authorised person who is also the contact person relating to an element of the European Critical Infrastructure,
- providing assistance to the competent central authority, especially data, documents and explanations necessary to:

- designate the element and its inclusion in the sector, as well as the removal of the element from the sector,
- assessment of the protection of the element, including ensuring protection of the element by the operator of the security service or armed security team,
- prepare a risk analysis of the sector,
- manage the registry of elements.

RISK MANAGEMENT AND PROCESSING THE SECURITY PLAN

Security plans are a tool to increase the security of critical infrastructure elements. Minimum procedure in the processing of the security plan is formulated in the Annex 2 of the Act No. 45/2011 Coll. on Critical Infrastructure and indicated in Figure 1.

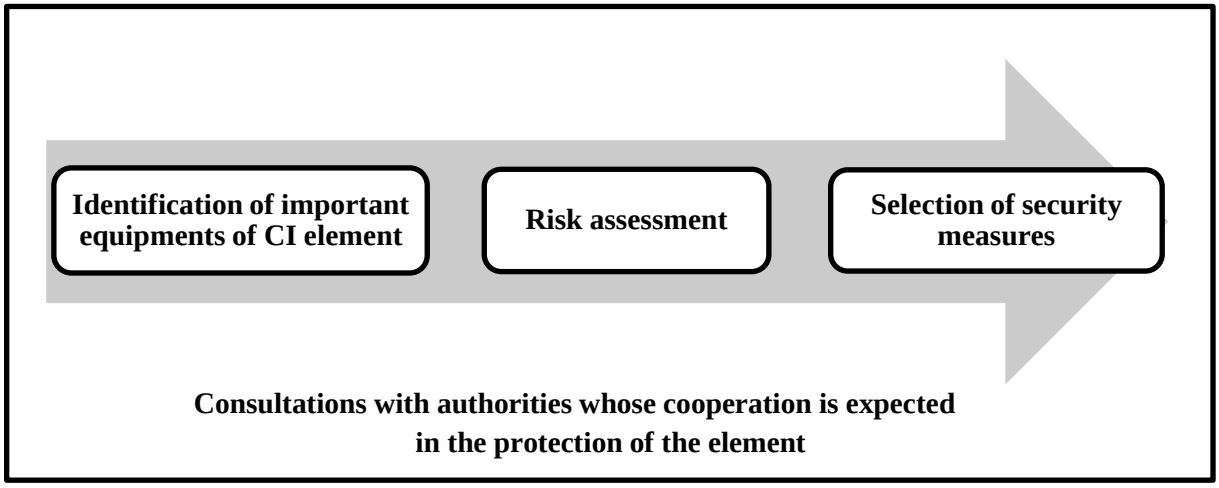


Figure 1. Minimum procedure in the processing of the security plan.

Minimum procedure in the processing of the security plan is closely related to the risk management process defined by ISO 31000:2009 which provides principles and generic guidelines on risk management. Relation between risk management process and processing the security plan is indicated in Figure 2. In this context, the individual steps of the security plan development can be described as follows:

- *Identification of important equipment of the CI element* – this phase relates to the analysis of the internal security environment of the critical infrastructure element. It aims to ensure reliable, up-to-date and relevant information on the situation and the state of the internal security environment, with emphasis on the threats needed to identify security risks. It includes an inventory of significant assets, in which it is necessary to include also the premises and objects of the whole organization, as well as significant assets, located in the individual spaces inside the buildings, which are called protected areas.
- *Risk assessment* – the overall risk identification process, risk analysis and risk assessment. When assessing the risks, the following key questions need to be answered:
  - What can happen and why?
  - What are the consequences?
  - What is the likelihood of their further occurrence?
  - Are there any factors that mitigate the risk consequences or reduce the risk likelihood?
  - Is the level of risk tolerable or acceptable and requires further treatment?

  Risk assessment allows managers and stakeholders to better understand the risks that could affect the achievement of objectives, their causes, consequences and the likelihood and effectiveness of risk management measures
- *Selection of security measures* – this stage applies to risk treatment. Risk treatment focuses on those risks that were not considered acceptable, i.e. their value is above the

acceptability limit. It consists of designing, adopting and implementing measures that influence their value in a selected way. Risk treatment methods may not necessarily be mutually exclusive or may not be appropriate in all circumstances. Risk treatment may create new risks or modify existing risks [4].

- *Consultations with the authorities, whose cooperation is expected in the protection of the element* – this stage covers communication and consultation as well as monitoring and review.

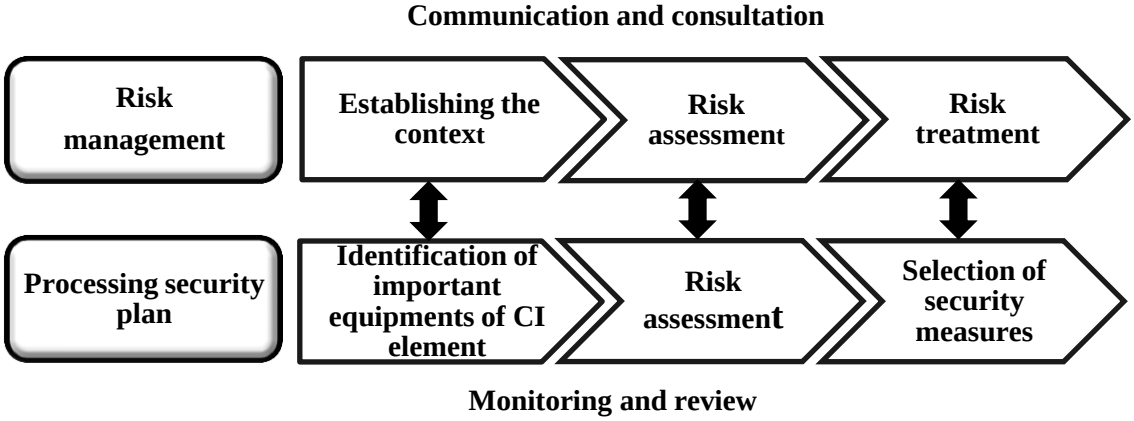


Figure 2. Relation between risk management process and processing the security plan.

Communication and consultation with external and internal stakeholders take place during the whole process of the security plan development. It is important that the staff responsible for the element protection and the stakeholders understand on what basis the decisions are taken and also to understand the reasons why certain activities are required.

Monitoring and review must include regular surveillance and periodic inspections, which may be periodic or ad hoc. Their goal is, e.g. to achieve more information to improve risk assessment, analyse events and learn from them, identify emerging risks, etc.

Risk management needs to be a continuous process since in day-to-day operations, incidents can undermine the best-laid plans and best-of-breed technologies [5, 6]. Security plans are a tool to increase the security of critical infrastructure elements. Their structure and scope is also formulated in Annex II of Council Directive 2008/114/EC. Together with the set of system measures of all actors involved in the management of the CI element and the intrinsic capabilities or properties of the element naturally resist the external and internal effects of the environment; they create conditions for achieving the resilience of the CI element [7, 8].

CONCLUSION

More than 90 % of CI in the SR is owned by private sector. It is evident that security cannot be just the responsibility of government but both the public and private sectors should work closely to adopt a more proactive approach to securing critical infrastructure. Close cooperation and exchange of information between all stakeholders is necessary to take into account the interdependencies between the CI elements and to identify the impact at the system level. It is important for owners and operators of CI to prefer the protection of critical infrastructure elements in terms of a safety and security to an economic point of view.

ACKNOWLEDGEMENTS

Preparation of this article was supported by the European Union within the FP7 project No. 608166 “Risk Analysis of Infrastructure Networks in response to extreme weather” and by VEGA grant No. 1/0240/15 “Process model of critical infrastructure safety and protection in the transport sector”.

REFERENCES

[1] Council of European Union: *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*.
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:01:EN:HTML, accessed 8th March 2018,

[2] –: *Act No. 45/2011 Coll. about critical infrastructure*.
http://www.zbierka.sk, accessed 8th March 2018,

[3] Hromada, M.: *Technological aspects of CIP in Slovak CI.* Ph.D. Thesis.
University of Zlin, Zlin, 2011,

[4] Leitner, B.: *General model for railway systems risk assessment with the use of railway accident scenarios analysis.*
Procedia Engineering **187**, 150-159, 2017,
http://dx.doi.org/10.1016/j.proeng.2017.04.361,

[5] Luskova, M. and Buganova, K.: *The importance of effective risk management system in the Slovak enterprises.*
WMSCI 2011 – The 15th world multi-conference on systemics, cybernetics and informatics. Orlando, International Institute of Informatics and Systemics, 2011,

[6] NTTSecurity: *Risk management is a continuous process.*
https://insight.nttsecurity.com/post/102dhyq/risk-management-is-a-continuous-process, accessed 8th March 2018,

[7] Hromada, M. et al: *System and way of critical infrastructure resilience assessment*.
UTB, Zlín. 2013,

[8] Rehak, D. et al: *European Critical infrastructure risk and safety management. Directive implementation in practice*.
Chemical Engineering Transactions **48**, 943-948, 2016,
http://dx.doi.org/10.3303/CET1648158.

Interdisciplinary Description of Complex Systems 17(1-A), 13-19, 2019

SECURITY OF SMART CITY

Richárd Pető*

Óbuda University
Budapest, Hungary

DOI: 10.7906/indecs.17.1.3
Regular article

Received: 21 June 2018.
Accepted: 31 December 2018.

ABSTRACT

If the topic is Smart City, we can talk about independent and several combined systems. Such systems may be for example energy saving and environment friendly vehicles, control system of traffic or up to date traffic information. Each system is in itself an important system, but if we connect them to a common network it can reduce significantly the operation time of tasks. What kind of events require complex operation or a system? Unfortunately, the increasing number of terrorist attacks can be heard in the news. Most attacks occurred against civilians in a place of mass occupancy. The perpetrators use cars and bombs to hit, blow up people. The article's aim is to review main problems of attacks and to describe a decision support system for coordination.

KEYWORDS

"Prophet" system, terrorist, map, security, coordination

CLASSIFICATION

JEL: F50

*Corresponding author, η: petorichard.mk@gmail.com; +36 30 9357667;
Haller str 20, 1096 Budapest, Hungary

INTRODUCTION

What is a smart city? Government decree 56/2017 (III. 20.) On the amendment of certain government decrees on the definition of the notion of 'smart city' and 'smart city methodology' " defines smart city as follows: "It is a settlement which plans and implements its integrated settlement development plan on the basis of the smart city methodology" [1; §5a], while smart city methodology is interpreted as follows: "The development methodology of settlements or groups of settlements, which advances the natural and man-made environment, digital infrastructure, the quality and economic efficiency of services with the use of modern and innovative information technologies in a sustainable fashion with the enhanced involvement of the population" [1, §5b].

In a city where the integration of systems of different functions operating fundamentally in an independent way is in focus and IT solutions are particularly highlighted. Such systems are, for example, BKK futár, Ch4llenge, Civitas Eccentric, Elliptic, Empower, Flow, Opticities, Smartlab etc. [2].

The construction and development of a smart city is a challenge not only in the field of technology but also in building and sustaining security. The mentioned systems contain data and information whose management must meet the requirements of the CIA (confidentiality, integrity, availability) and they must not be accessed by any unauthorised person. Unfortunately, an increasing number of terrorist attacks are carried out. In these cases, the number of attacks aimed at natural people is extremely high and this trend is further growing. Recently it is the series of vehicle-ramming attacks that can be recalled on the basis of the news. Browsing the databases of terrorist attacks, it can be seen that the number of cases registered annually was below 8 between 1970 and 2013 while this value is between 25 and 50 in the years 2014 to 2016 [3].

What can be the consequences of a vehicle-ramming attack?

In July 2016 a cargo truck was driven into the crowd celebrating Bastille Day on Promenade des Anglais in Nice, resulting in the death of 86 people and the injury of hundreds [4]. In August 2017 a Fiat van was driven into the crowd in a pedestrian street of Barcelona La Rambla, frequented by tourists. The damaged van moved along the street for 530 metres. The casualty list is: 1 killed and 88 injured [5].

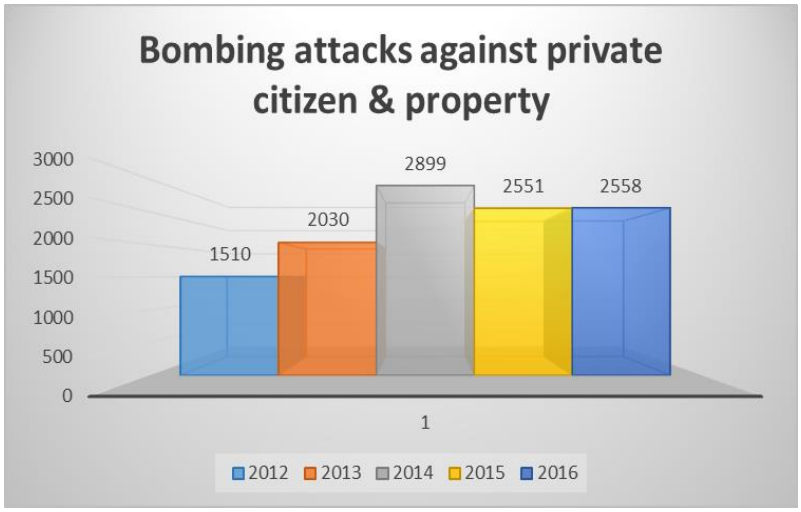


Figure 1. Bombing attacks against private citizen & property between 2012 and 2016 [6].

Defence against bomb attacks comprises a special branch of property protection, requiring continuous development and renewal. Its special features are clearly illustrated by the fact that the organisation and installation of the defence are aimed at the preparation for an atypical, unusual event or series of events. An explosion or the impacts of a blast fall into the category of extreme incidents whose severity is further aggravated by the intentional nature of the committed act, and the fact that such acts may be targeting either pre-selected people or objects, or randomly chosen people or objects anywhere in the world and at any time [7]. "The estimation of the risk of a particular terrorist act requires the coordinated work of a lot of fields of expertise. The cooperation of the experts of several independent areas (security policy experts, intelligence officers, engineers, mathematicians, etc.), and a sufficient amount of information are needed for estimating the risks related to one particular threat" [8].

The identification of risks is only the first step of planning the defence because it does not provide efficient defence. Effective defence is provided with the combined use of active and passive mechanical devices, electronic signalling systems (and protection systems), action plans, and regulation strategies. There is no doubt that the determination of action plans and regulation strategies requires a significant planning capacity, especially when there is a need for the concerted cooperation of several organisations. In the case of a bomb attack the coordinated cooperation of disaster management, national defence, civil protection, ambulance, and law enforcement agencies should be continuously provided during the prevention, countering, and the damage elimination. For professional planning and timing of the tasks the multi-faceted analysis of the dangers (intention to attack, methodology; used devices, materials, preparations, damage assessment of momentary dangers and further risks, the methods of their prevention and elimination, etc.) and the seamless and continuous information exchange among organisations with different responsibilities and philosophies are inevitable. Below the author partially presents a map-based system planned by him, which facilitates the cooperation of the services and agencies responsible for countering the above-mentioned threats as the execution of their tasks may be timed and tracked, independently of the local knowledge of the person coordinating the variety of agencies.

THE "PROPHET" SYSTEM

To determine the requirements and structures of a decision support system proved to be an extremely complex task. The first step was the identification of the exact goal of the system, the range of its application, and the requirements of its structure. What made the task very difficult was the fact that the knowledge from each field of expertise had to be integrated. They were mostly interrelated or even complemented each other although in some other cases there was no relation amongst them. In the author's opinion the transparency of the "Prophet" system requires knowledge in the following special fields: safety science, blasting technology, fire protection, labour safety, architecture, disaster management, law enforcement; IT, telecommunications, electrical engineering, cartography, law and psychology [9].

PREVENTIVE MEASURES

What measures are to be taken? What should be the order of steps in situation management? The system I planned includes the following. As the first step, significant data and information related to the area should be clearly seen. If they are at our disposal, the system can provide a comprehensive picture of what is endangered and of the possible losses. Second, a thorough study of the region and local crime statistics is necessary. These data are supposed to show the number and type of attacks and also the time of the day and the most common targets and additional special details. From these data the most potential threat may

be determined. Upon performing this study, a vulnerability assessment of the facility or building is to draw; then the estimate of the risk of attack must be made. The security plan should be made on the basis of the vulnerability assessment and it is to assure that security plans are appropriate and suitable for the protection of the area.

It is extremely important, that the plan has to be regularly updated. A formal security plan review should be performed once a year. The security plan should be modified if a significant change is introduced in the organization or if an attack occurs [7]. Past incidents and standards help in choosing the right methods. In most situations the goals are unattainable, though.

After the assessment of the data, information, dangers, and risks relating to an area, the planning of prevention, protection, and damage control activities can be launched.

Imagine a crowded city where schools, hotels, supermarkets, residential buildings, car parks are close to each other. In most cases the old buildings are built on very narrow lanes, and there is no or hardly any space between them. Another problem arises due to roads and means of public transport. Roads and electric wires are similarly close to the buildings.

One can see in Fig.2 three buses and two trams which are close to buildings of mass occupancy. A well-parked vehicle carrying hundreds, or thousands of pounds of explosive can strongly increase the vulnerability of the area. Why is space so important? Table 1 includes the main reasons.

Figure 2. Insufficient separations among the education institute, apartment buildings and means of public transport.

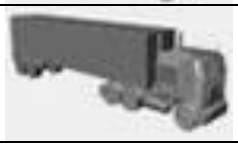
An exploding car bomb or truck bomb also known as a Vehicle Borne Improvised Explosive Device (VBIED) kills people inside the building, outside in the street and may collapse nearby buildings by blast wave and fragmentation.

THE OBJECTIVES OF THE *PROPHET* SYSTEM

The brief summary of the objectives of the system:

- primarily to provide support to decisions made about the management of explosion threats, and to increase the efficacy of the execution of tasks (including those conducted in mission areas),
- the identification of the potential location of a bomb attack in the most precise way possible,
- estimation of relating risks,
- estimation of the (human and technical) resources of the involved organisations in relation to the particular task (intelligence, prevention, defence, counteractions, damage control),

Table 1. Bomb threat stand-off distances [7].

Threat Description		Explosives Capacity (TNT Equivalent)	Mandatory Evacuation Distance*	Preferred Evacuation Distance**
	Pipe Bomb	5 lbs/ 2,3 kg	70 ft/ 21 m	1 200 ft/ 366 m
	Suicide Vest	20 lbs/ 9,2 kg	110 ft/ 34 m	1 750 ft/ 518 m
	Briefcase/ Suitcase Bomb	50 lbs/ 23 kg	150 ft/ 46 m	1 850 ft/ 564 m
	Sedan	500 lbs/ 227 kg	320 ft/ 98 m	1 900 ft/ 580 m
	SUV/Van	1 000 lbs/ 454 kg	400 ft/ 122 m	2 400 ft/ 732 m
	Small Delivery Truck	4 000 lbs/ 1 814 kg	640 ft/ 195 m	3 800 ft/ 1 159 m
	Container/ Water Truck	10 000 lbs/ 4 536 kg	860 ft/ 263 m	5 100 ft/ 1555 m
	Semi-Trailer	60 000 lbs/ 27 216 kg	1 570 ft/ 479 m	9 300 ft/ 2 835 m

*Governed by the ability of typical US commercial construction to resist severe damage or collapse following a blast. Performances can vary significantly, however, and buildings should be analysed by qualified parties when possible.

**Governed by the greater of fragment throw distance or glass breakage/falling glass hazard distance. Note that pipe and briefcase bombs assume cased charges that throw fragments farther than vehicle bombs.

- coordination and the streamlining of the coordination of the work (intelligence, prevention, defence, counteractions, damage control) of the relevant organisations,
- synchronisation of the activities of service-providers in coordination with the special services,
- as a secondary tier: to provide support to decisions relating to the management of any other threat or disaster, and the increase of the efficacy of the execution of tasks.

The estimation of the destructive effect of an explosive device in a precisely determined location. This article provides the description of the estimation of the destructive effect of an explosive device planted or positioned in a precisely determined location [10].

THE ESTIMATION OF THE DESTRUCTIVE EFFECT OF AN EXPLOSIVE DEVICE IN A PRECISELY DETERMINED LOCATION

The location of the explosive device (VBIED) planted by a bomber is precisely known. It may be disclosed on the basis of the information provided by the bomber or another person – a passer-by, security guard, etc. The advantage of the situation is that it is easier to estimate the extent of the danger zone. In the simulated attack the vehicle in question falls into the van category, the relating values in the security table are 120 m and 730 m. As the next step the perimeter of the danger zone can be determined through the comparison of the two parameters follows with the location scheme. The damage assessment of installations is based on determined building classifications, people inside, evacuation time, and other dangers. The map section below illustrates various object classifications. Apart from objects vehicles, means of transportation, public services, telecommunication networks, and other infrastructures other on surface and underground should also be taken into consideration. If the necessary data are arranged into a data table, a complex system takes shape which almost immediately provides the necessary information (Fig. 3).

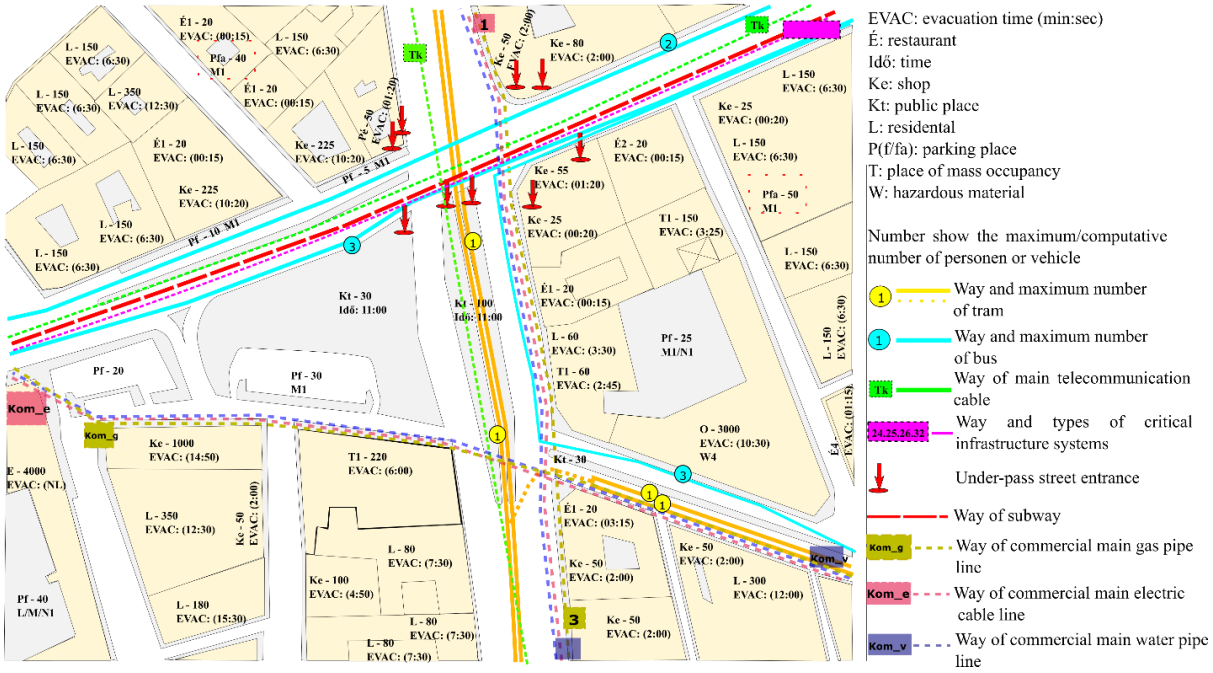


Figure 3. The scheme of all data of the *Prophet* system.

When all the necessary information is available damage assessment will follow. It involves the comparison of the given scheme of the scene – with all information displayed – and the perimeter of the danger zone. For damage assessment purposes the areas within the circles are to be analysed. The completed analysis will clearly indicate which organisation or service provider is to be alerted for the prevention or elimination of the damage or loss in the case of injuries. The efficacy of the measures taken is further increased by simulated and elaborated scenarios.

CONCLUSION

Any explosive device may cause huge destruction in the split of a second. This is particularly true for VBIEDs. The more densely populated an area is or the larger temporary population it has, the more developed infrastructure it has, the bigger the caused damage, and the larger the number of injured and the losses of lives are. Perhaps one of the best-known bomb attacks was committed against the USA Embassy, located along a busy road in the centre of Nairobi, the capital city of Kenya. The seven-story building next to the Embassy collapsed and the

Embassy buildings turned unusable although remained intact. The terrorist attack committed with the use of an explosive device planted in a Toyota Dyna van claimed more than 200 lives and more than 4 000 people were injured by the blast. The described *Prophet* decision system may significantly help discovering bombing incidents against population. Even if detection has not been successful it may assist to process of precedence, prevent and recovery. Factories need to have own security and emergency plans in case of accidents and terror attacks. Factories also need to cross-check with the competent Police Authority and National Directorate General for Disaster Management. The "Prophet" system complements other decision support systems and makes more efficient and resilient [11] those performance of management processes between population, authorities and company.

REFERENCES

[1] –: 6/*2017. (III. 20.) Government Decree amending certain government decrees concerning the definition of "smart city", "smart city methodology"*.
https://net.jogtar.hu/jogszabaly?docid=A1700056.KOR&timeshift=fffffff4&txtreferer=00000001.TXT, accessed 13th March 2018,

[2] Lechner Knowledge Centre: *Smart City.*
http://okosvaros.lechnerkozpont.hu/hu, accessed 13th March 2018,

[3] Global Terrorism Database: *Vehicle attack.*
http://www.start.umd.edu/gtd/search, accessed 13th March 2018,

[4] –: *Pedestrians hit by vehicle in Flinders Street.*
https://index.hu/kulfold/2017/12/21/ausztralia_tomeg_auto_gazolas, accessed 13th March 2018,

[5] –: *Barcelona attack: 13 killed as van rams crowds in Las Ramblas.*
https://24.hu/kulfold/2017/08/17/tomegbe-hajtott-egy-furgon-barcelonaban, accessed 13th March 2018,

[6] Global Terrorism Database: *Bombing attacks against private citizen and property*.
https://www.start.umd.edu/gtd/search/Results.aspx?&start_year=2016&start_month=1&start_day=1&end_year=2016&end_month=12&end_day=31&asmSelect0=&asmSelect1=&weapon=6&attack=3&target=14&dtp2=all&success=yes&casualties_type=b, accessed 24th January 2018,

[7] Pető, R.*: Defence and evacuation problems of building for masses*.
International Conference on Military Technologies, 22-23 May 2013. Faculty of Military Technology, University of Defence, Brno, 2013,

[8] Pető, R.: *Stochastic Methods for Risk Analysis of Explosive Acts*.
In: *Methods, possibilities and means of enhancing the protection of permanent buildings against explosive acts (design guide)*. National University of Public Service, Budapest, Ch.4, 2013,

[9] Pető, R.: *The "Prophet" decision support system.*
Procedia Manufacturing **22**, 1023-1030, 2018,
http://dx.doi.org/10.1016/j.promfg.2018.03.145,

[10] Pető, R.: *Tools for protecting objects and opportunities for blasting / terror blasting*.
Óbuda University, Budapest, 2017,

[11] Flammini, F., ed.: *Resilience of Cyber-Physical Systems.*
Springer International Publishing, Heidelberg, 2019,
http://dx.doi.org/10.1007/978-3-319-95597-1.

Interdisciplinary Description of Complex Systems 17(1-A), 20-25, 2019

UNIFIED ASPECT SEARCH ALGORITHM

Attila Albini[1,] *, Gyula Mester[1] and László B. Iantovics[2]

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

[2]Petru Maior University, Department of Informatics
Tirgu Mures, Romania

DOI: 10.7906/indecs.17.1.4
Regular article

Received: 14 November 2018.
Accepted: 31 December 2018.

ABSTRACT

Man does the studying of systems by modelling it. Examining parameters which are describing the operation of the system is important when creating the model. The parameters required for the test are retained and the irrelevant parameters are discarded. The remainder of the model determines the aspect system of the examination. The system can be tested according to many of the disciplines. These aspect systems are not uniform. For this reason, the product of the examinations by different disciplines is difficult to compare. Placing examination on uniform basis could provide common foundation for a single modelling process. In this article an aspect search algorithm is created which is based on the philosophical topics. All disciplines can be derived from philosophy. Because of these examinations based on philosophy can be uniform. The results of the tests are comparable. The requirements for the examination can be standardized. In addition, this method makes easier to adapt the operation. For example, the operating principles of energetic, mechanical, IT and social organizations can be adapted to each other.

KEYWORDS

system, examination, aspect, search, algorithm

CLASSIFICATION

ACM: H.1.1
JEL: D83
PACS: 01.70.+w

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

INTRODUCTION

Man tries to understand the operation of nature, and then tries to change it according to the needs. The purpose of intervention in nature is to ensure the sustainability of human civilization. In order to understand the operation of nature and to solve problems, one observes surroundings, forms a model, specifies operational rules and then uses the results in real life [1]. A critical part of the process is creating the model. Reality is a very complicated system with many connections. Thus, modeling can only partially be solved [2]. The system components required to identify the problem are taken into account when designing the model. The unnecessary elements are omitted from the examination. The model is a virtual copy of the system. In this model one can carry out studies that should interfere with the operation of the original real system or should cause its transformation [3-6]. The validity of the model used for the examination requires minimization of subjectivity. To this end the criteria system of the competent disciplines is applied. However, the aspect system of the disciplines is not uniform. For this reason the results of the examinations are difficult to compare. By using a unified criteria set these problems can be alleviated. Since all disciplines can be derived from philosophy the examinations are based on philosophy can be uniform [7]. A unified method can be useful to investigations for technical and human systems, too.

This article contains a new algorithm based on philosophical foundations. The purpose of this algorithm is to produce a unified aspect system for analysis. Then this aspect system can be used as the starting point for modeling. Thus the basis of the examination becomes homogeneous. The results of the examinations carried out on this basis are comparable with each other. Finally in the study there is an example for use.

PRINCIPLE OF OPERATION

The algorithm can be used in two steps. First the general logical aspect system of the given examination can be produced. Subsequently the relevant aspects of the specific system can be determined. If the general aspect system of an examination type has already existed then only the second step is to be performed. The first step of the algorithm has three procedures: dimensioning, scaling, evaluating. In the second step – when applying the algorithm to a specific system – the relevant aspects of the aspect groups should be applied.

Philosophical topics are the source poles in the procedure. Every dimension of the algorithm must be derived from the poles according to the orientation of the examination. The scaling of the created n-dimensional space should be granulated according to the details of the test. The resulting n-dimensional finite space can be interpreted as a discrete function whose value set is the Cartesian product of the scale values. Each function value defines a general aspect group. This is how the general logical aspect system of the test produces.

PHILOSOPHICAL POLES

To use this algorithm, the topics of philosophical basic questions are considered as source points. This ensures a unified foundation. The main philosophical themes [8], their equivalent elements in the algorithm and the methods of determining aspects are:

- examination of existence: What is the purpose of being? How can continuity of existence of individuals or groups be ensured? What are the conditions for this? In the algorithm the equivalent element of this question group is the pole of existence. The relevant aspects should be determined by examining components affecting existence. The recommended methods are the study of effect time and the study of impact size [9],
- examination of knowledge: Is the structure of the system known to the extent required for modeling? How much subjectivity can be allowed for the examination of the system? In

the algorithm the equivalent element of this question group is the pole of structure. To determine the aspects the human abstraction layers and the natural layers can be tested [8],

- examination of acting: What determines the actions, operations, and functionality of the systems? How can this be modeled? What features can be identified in the functioning of individuals and groups? In the algorithm the equivalent element of this question group is the pole of function. Relevant aspects can be found by studying the features of the system. The recommended method is to find equivalency with the abstract categories of human thinking [8],
- examination of truth: Which allegation is true? What are the subjective and objective elements of truth? Is there objective truth? What kind of truth determines the validation of the system operation? How to model the first level change of systems (statogenesis)? In the algorithm the equivalent element of this question group is the pole of control [8]. In order to determine the aspects measurement, validation and control topics should be studied [3-6],
- examination of changeability: What is organic change (morphogenesis)? What system components determine the possibility and course of change? How can it be modeled or influenced? In the algorithm the equivalent element of this question group is the pole of change. This includes all the aspects that affect system change and flexibility of the system [1, 7].

The general poles (Fig. 1.) are: *existence*, *structure*, *function*, *control*, *change*.

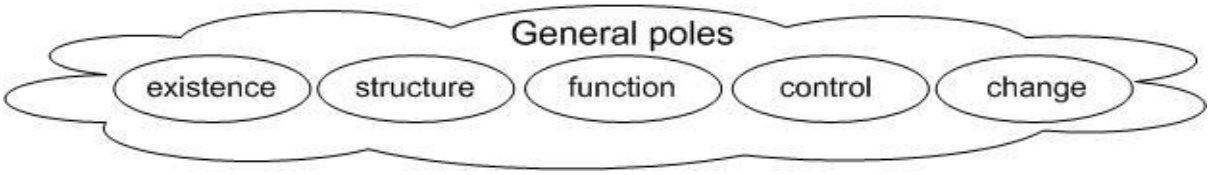


Figure 1. General poles based on philosophy.

DIMENSIONING AND SCALING

Prior to conducting the test, its spectrum and orientation shall be indicated. It is necessary to analyze which elements are relevant and how detailed they will be in the modeling. Dimensions and scaling of the algorithm must be established based on these. The following should be considered:

- if the system needs to be examined from a number of independent aspects in more detail within a given pole, then a separate dimension per every aspect should be extended from the pole. This can be called branched extension,
- if there is only one aspect by a given pole then that particular pole should be extended to a dimension. This can be called a normal extension,
- if a given pole can be characterized by a single scale value, then this pole will not have an independent dimension. At the end of this process such scale values can be merged into a dimension. This can be called merged extension,
- poles that are not relevant to the whole test should not be included in the modeling. From such poles there will be neither dimension nor scale value. This can be called pole irrelevance.

Dimensioning is shown in Figure 2. Scaling and granulation follows dimensioning. It is necessary to determine the scale values of every dimension. Details of modeling can help to do this. The poles extended to single scale value should be merged in a common dimension. This common dimension can be an extended dimension of an independent pole.

EVALUATION

The finite discrete space created after the above operation should be interpreted as a function. The output value of the function for a given spatial point is the list of appropriate scale

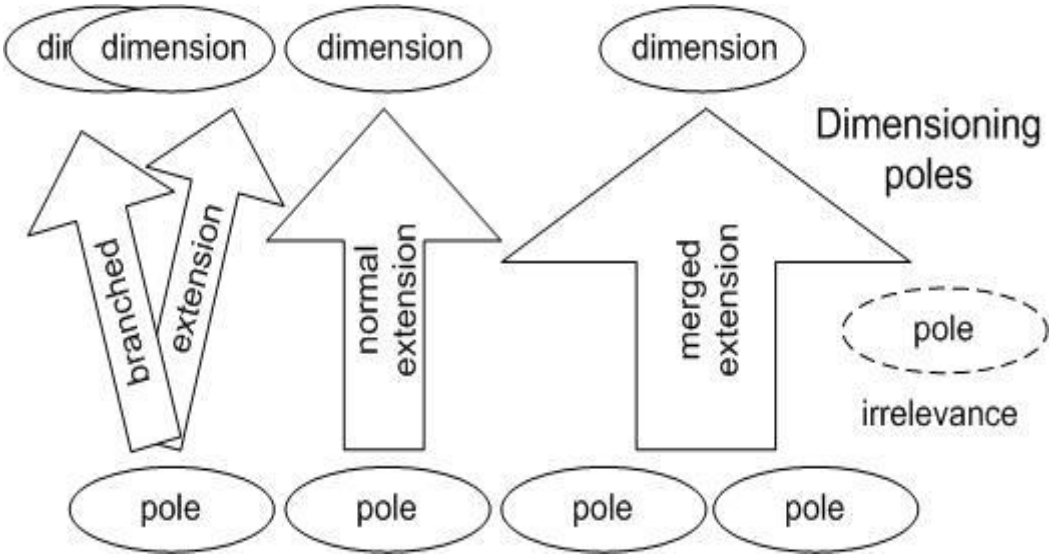


Figure 2. Dimensioning.

values. Thus, the value set of the function is the Cartesian product of scale values of dimensions.

The whole value set should be determined during the evaluation. The function values must be interpreted in a text-read way and extend them to sentences. This method creates the general logical aspect system. The number of the general logical aspect groups that are emerging is equal to the product of numbers of scale values. According to these aspect groups one can examine the concrete system. When applying the algorithm to a specific system the relevant aspects of the aspect groups are to be produced. This can lead to thousands of aspects of the examination depending on the complexity of the system.

EXAMPLE FOR USE

In the following example IT clouds are examined from IT security aspect. The simplified general logical aspect of the study is generated by the algorithm. The emphasis is on examining technological and natural effects [8].

Each pole is used to produce the spatial structure. The scale values of existence dimension are determined according to the elements of the security paradigm [9-10]. The scale values of structure dimension are identified on the basis of layer structure of the cloud [8-9,11]. The scale values of function dimension are equivalent to the elements of the infocommunication paradigm [8]. The control and change poles are represented only by scale values which are added to the function dimension [3-4].

In this way a 3-dimensional space is formed (Fig. 3.). Dimensions and scale values are:

- security dimension {availability, integrity, consistency (derived from confidentiality)},
- structural dimension {fundamental-, hardware-, virtual-, operational-, management-layer},
- functional dimension {storing, transforming, transmitting, control, changeability}.

This method has a total $3 \times 5 \times 5 = 75$ general logical aspect groups. By the end of the specific evaluation, the complexity of the system can lead to hundreds of specific aspects for the study.

CONCLUSIONS

System examinations are based on modeling. Generating a model is not easy, because reality is complicated [1-2]. In addition, the aspects of the disciplines are not uniform and the tests are often multidisciplinary. Therefore the production of the criteria system is a complex problem

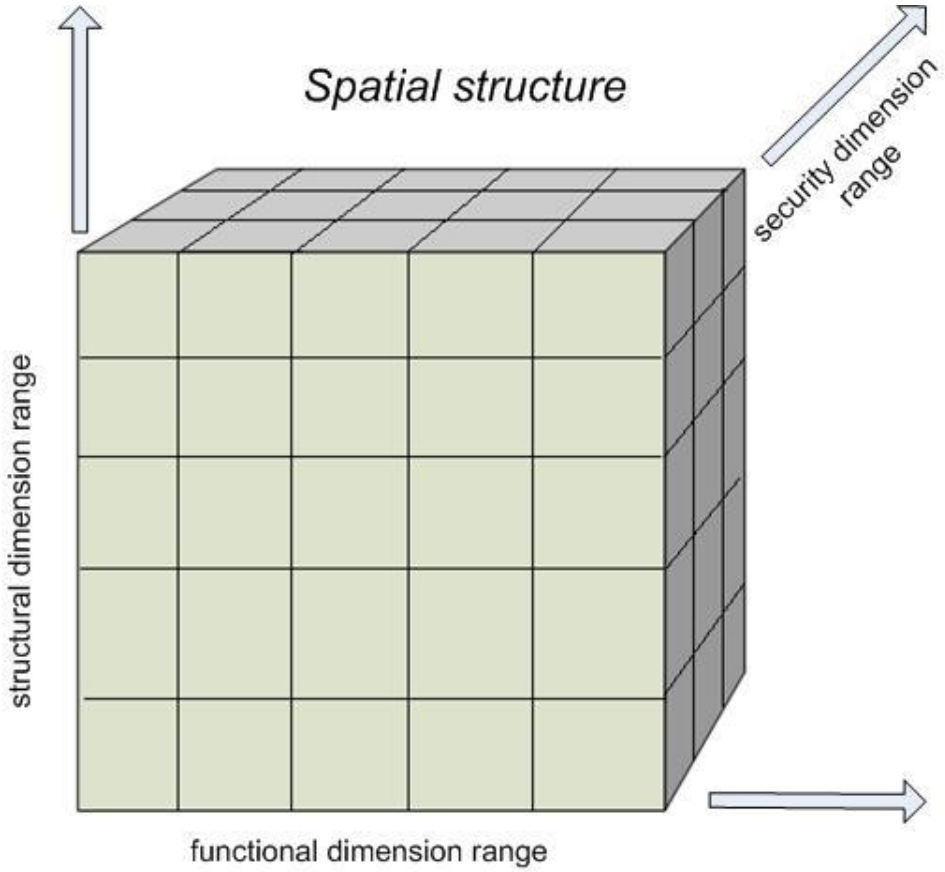


Figure 3. Spatial structure used for the example [8].

The previously described algorithm produces the aspect system of examination. The algorithm rests on philosophical basis. Philosophy is the ancestor of disciplines so the criteria system can replace the aspect system of the various disciplines in a uniform way [7]. Following the identification of the examination aspect system the system model is easier to create.

The starting points of the algorithm are the main philosophical themes. The boundary conditions, the orientation, and the need for details determine the algorithm. This allows to create a general logical system of criteria that is appropriate to the needs. Using this, the relevant aspect system can be produced. The example mentioned in this study confirms the usability of the algorithm.

This modeling is based on unified principles. Because of this the results of the tests are comparable [7]. In addition, this method makes easier to adapt the operation. For example, the operating principles of energetic, mechanical, IT and social organizations can be adapted to each other.

ACKNOWLEDGEMENTS

The research on which the publication is based has been carried out within the framework of the project entitled “The Development of Integrated Intelligent Railway Information and Safety System” (Application number: GINOP-2.2.1-15-2017-00098).

REFERENCES

[1] 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,

[2] Rajnai, Z. and Vanderer, G.: *Applicability of risk-evaluation theories in crtitical infrastructures.*
Bolyai Szemle **2014**(2), 75-84, 2014,
[3] Mester, G.; Pletl, S.; Pajor, G. and Rudas, I.: *Adaptive Control of Robot Manipulators with Fuzzy Supervisor Using Genetic Algorithms*.
In: Kaynak, O., ed.: *Proceedings of International Conference on Recent Advances in Mechatronics.* Istanbul, 1995,
[4] Iantovics, L.B. and Zamfirescu, C.B.: *ERMS - An Evolutionary Reorganizing Multiagent System*.
International Journal of Innovative Computing, Information and Control **9**(3), 1171-1188, 2013,
[5] 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,
[6] 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,
[7] Yingchun, L.: *A systems-science-based knowledge explanation method*.
Tsinghua Science and Technology **6**(1), 49-56, 2001,
[8] Albini, A.; Tokody, D. and Papp, J.: *IT Infrastruktúra Informatikai Biztonsági Aspektusai – IT Security Aspects of IT Infrastructure*. In Hungarian.
Bánki Reports **1**(1), 11-16, 2018,
[9] Kovács, Z.: *Cloud Security in Terms of the Law Enforcement Agencies*.
Hadmérnök **7**(1), 144-156, 2012,
[10] Rajnai, Z. and Rubóczky, E.S.: *Moving Towards Cloud Security*.
Interdisciplinary Description of Complex Systems **13**(1), 9-14, 2015,
http://dx.doi.org/10.7906/indecs.13.1.2,
[11] Albini, A. and Rajnai, Z.: *General Architecture of Cloud*.
Procedia Manufacturing **2018**(22), 485-490, 2018,
http://dx.doi.org/10.1016/j.promfg.2018.03.074.

Interdisciplinary Description of Complex Systems 17(1-A), 26-39, 2019

DATA TRANSFER RATES AND DATA TRAFFIC TRENDS ON MOBILE NETWORKS

Zsolt M. Temesvári* and Dóra Maros

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

DOI: 10.7906/indecs.17.1.5
Regular article

Received: 11 July 2018.
Accepted: 31 December 2018.

ABSTRACT

This article intends to demonstrate – through the monitoring of traffic data – the importance of data transfer rate on mobile networks and prevalent user trends. Current paper examines both already operating mobile networks and ones presently in the state of standardization in order to shed light on the data transfer rate maximizing strategy, and to find out how a wide frequency spectrum should be necessary for handling growing user demands. Furthermore, recognizing the demand for the continuous expansion of data traffic, current article – relying on previous Cisco research and the analysis of broadband mobile networks – aims to estimate the necessary data transfer rate and the amount of increase in data usage regarding the next few years to serve the developing mobile technologies. In the world of IoT, M2M and Smart Cities, the available mobile networks most likely will not be able to sufficiently deal with the high traffic, the article seeks to answer whether the development of new mobile technologies (like the 5G) are in line with the growing needs of users and machines and to propose a solution for handling the expected data traffic.

KEY WORDS

data traffic, data transfer rate, trends, growing needs

CLASSIFICATION

JEL: L86

*Corresponding author, η: zsolt.temesvari@gmail.com; +36 30 7771713;
H –1428, Budapest, Pf.:31, Hungary

INTRODUCTION

Demand for technological progress regarding the mobile networks is ever increasing. Thanks to the advancement of mobile technologies, user needs can be properly served. The position of frequency spectrum defines the possibilities of wireless technologies regarding the ensured coverage and quality, including the maximum available data transfer rate. The service providers have made huge efforts in the last few years to maximize data transfer rate and make the 4G (LTE) network available – including suburban and rural areas as well – since they already have the necessary frequencies to build a nationwide coverage. The LTE-Advanced and the upcoming 5G (that is still under standardization) is capable of a very high speed. But, is that rapid innovation, high data rate and huge capacity really necessary? This article is about to answer this question by presenting the LTE-Advanced and the 5G networks, and by analysing forecasts and showing trends of mass events and cities from a live mobile network point of view. The processed sampling data came from a mobile network of a service provider that has millions of users.

FREQUENCY BANDS FOR 4G (LTE) IN HUNGARY

The frequency is the basis of mobile services, having the appropriate frequency bands is fundamental to radiate mobile technologies, thus it has a key role in radio communication. It should be also taken into account that the frequency bands are exclusively allocated to specific services, which is a limitation of frequency resources. Cutting-edge technologies or creating new services increase the demand for wider frequency spectrum [1].

Mobile operators usually lease the frequencies on a long-term basis through a frequency tender issued by the Government. The last frequency auctions of Hungary took place in 2014, when 280 MHz frequency spectrum was announced for HUF 104,15 billion to be undertaken for 20 years. The purchasable frequencies were made public in packets, blocks “A”, “B” and “C” had the 800 MHz, the 900 MHz and the 2 600 MHz band, blocks “D”, “E” and “F” contained the 1800 MHz frequency band, block “G” offered the 2 600 MHz FDD band, while in block “H” the 2 600 MHz TDD could be purchased [2, 3]. The 800 MHz band became disengaged due to the disconnection of analogue TV broadcast [4]. This band is the most significant in respect of coverage, since the propagation of radio signals is more favourable in this band than in higher ranges.

During the auction, service providers entered successful bids in a total value of HUF 130,6 billion and acquired lease rights for the frequency bands for 20 years, and accepted other criteria as well: for instance the 4G service must be available for 96 % of the population and cover at least 90 % of Hungary’s territory within 60 months. All operators (which provide mobile services) got frequency band on 800 MHz, 900 MHz and 2 600 MHz. The 800 MHz and 2 600 MHz bands play a role in extending the 4G service, the 800 MHz band is essential to achieve nation-wide coverage. The successful frequency auction was a milestone of Hungarian mobile telecommunication and defined the long-term strategy of wireless service providing companies. The sold bands are shown in Fig. 1.

Hungary’s next frequency auction will take place in the coming years. The most important band that could be purchased through this tender is the 700 MHz spectrum. This band will likely be used for the LTE-Advance (and possibly in the future for the 5G), in conjunction with the neighbouring 800 MHz and later on the 900 MHz bands [5].

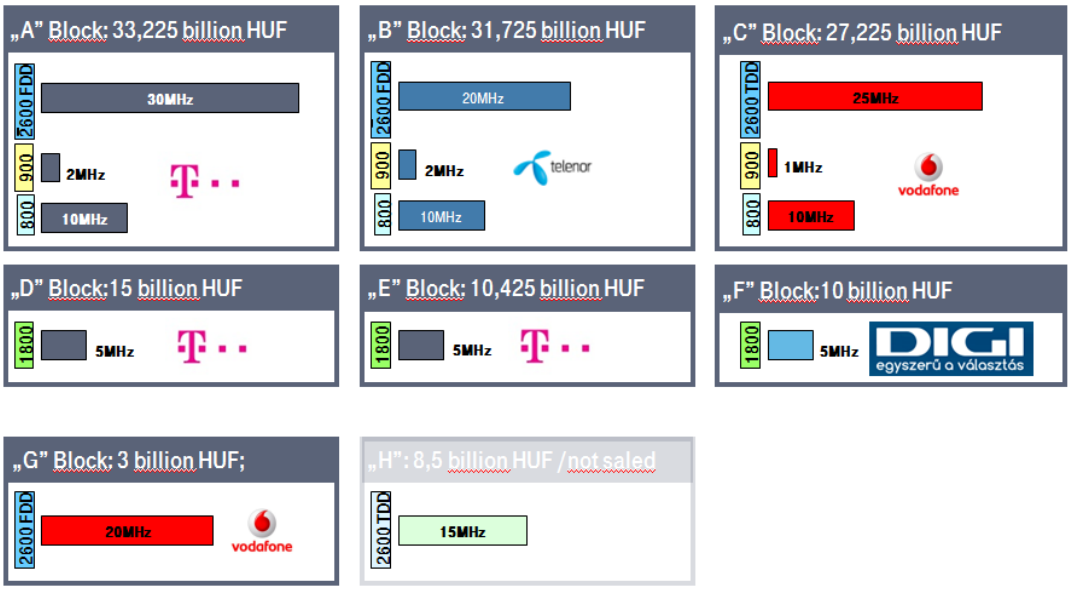


Figure 1. The sold bands of Frequency Auction Hungary 2014.

BROADBAND MOBILE NETWORKS

4G (LTE) PLANNING STRATEGY TO MAXIMIZE DATA TRANSFER RATE

The 4G is a single-frequency wideband network, which means that each mobile cell of a base station interferes with each other and with the surrounding base stations (and with their cells) as well. This considered, the dominance of mobile cells should be increased in their respected service area as much as possible, in order to achieve the theoretically available maximum speed. Increasing dominance and reducing interference will result in an improvement of SNR (signal-to-noise-ratio), which directly affects the data transfer rate. Therefore the mobile operators design their networks in the line with this strategy [6, 7]. The following diagrams indicate the importance of SNR and the reduction of available data transfer rate due to SNR degradation close to the boundary of cells (sectors).

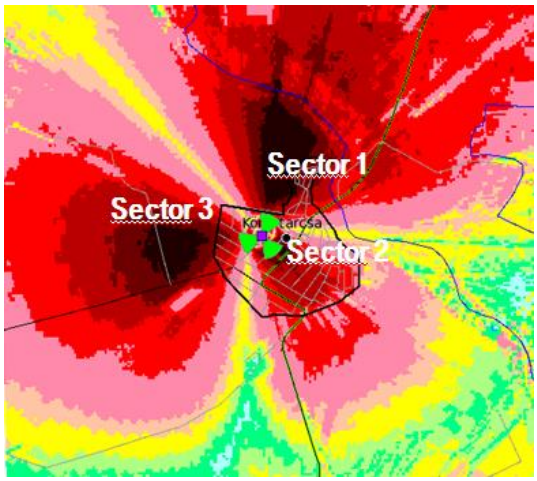


Figure 2. The available data transfer rate within the three cells of a base station (the darker the area, the higher the available speed – the data transfer rate is the minimum at the boundary of the cell's range).

In Fig. 2, mobile sector 2 is rotated to the direction of sector 3. The two cells operate on the same frequency, which increases the interference and damages SNR in both cells (in sector 2 and 3), thus the available data transfer rate is also getting lower [7].

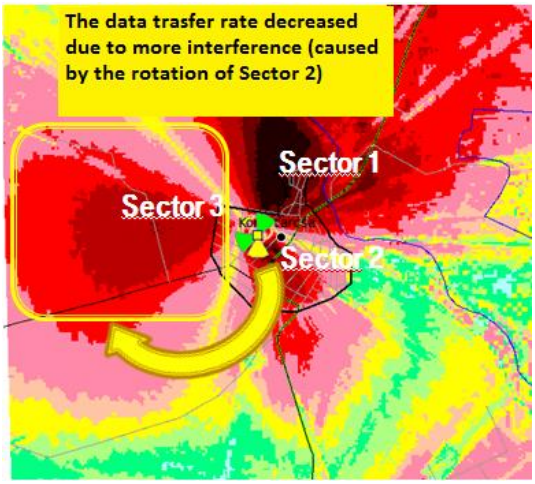


Figure 3. The available data transfer rate within the three cells of a base station (the darker the area, the higher the available speed) – after the rotation of sector 2 to the direction of sector 3.

THEORETICAL DATA TRANSFER RATES ON LTE-ADVANCED IN HUNGARY

The 4G service has been available in Hungary since 2012 and operated on the 1800 MHz band with 10 MHz bandwidth, which was capable of reaching ~75 Mbps [8] theoretical maximum data transfer rate by using MIMO (Multiple Input Multiple Output – multiple antenna is in use on the transmitter and receiver side) [7]. Following the successful frequency auction, the Hungarian operators could multiply the available speed on their 4G network since the end of 2014 due to the new frequency bands (800 MHz and 2 600 MHz) and the fact that the bandwidth was increased on 1800 MHz.

The LTE-Advanced refers to the data transfer rate of over 150 Mbps, which was switched on in Hungary in 2014 and has been available nation-wide since 2015. LTE-Advanced could be described as a combination of available frequency bands, which means that separated bands can be aggregated using the so-called „carrier aggregation" feature. For example if a 20 MHz wide frequency band provides 150 Mbps theoretical maximum download speed and there is an additional 20 MHz bandwidth aggregated to our bandwidth, the maximum download speed will be doubled, reaching 300 Mbps and the capacity will increase as well [9].

As mentioned above the double carrier aggregation is already in operation in many parts of Hungary. The triple carrier aggregation was introduced in November 2016 in Hungary, when the 800 MHz (20 MHz wide band), the 1800 MHz (20 MHz wide band) and the 2 600 MHz (20 MHz wide band) frequencies were merged in order to reach the theoretical maximum download speed of 450 Mbps (with 60 MHz wide spectrum). The maximum download data transfer rate of LTE-Advanced technology are summarized on the following diagram.

Later on the so-called Massive MIMO will be released, which provides much more than 2×2 antennas on the transmitter and receiver side [11], the theoretical maximum downlink data transfer rates could be also seen in Fig. 4.

5G EXPECTATIONS FROM A DATA RATES POINT OF VIEW

Standardization of the fifth-generation mobile network (5G) is currently under way. All the relevant mobile base station manufacturing companies and the major players on telecommunications market are involved in this collaborative effort. The first release is expected in 2020 [12].

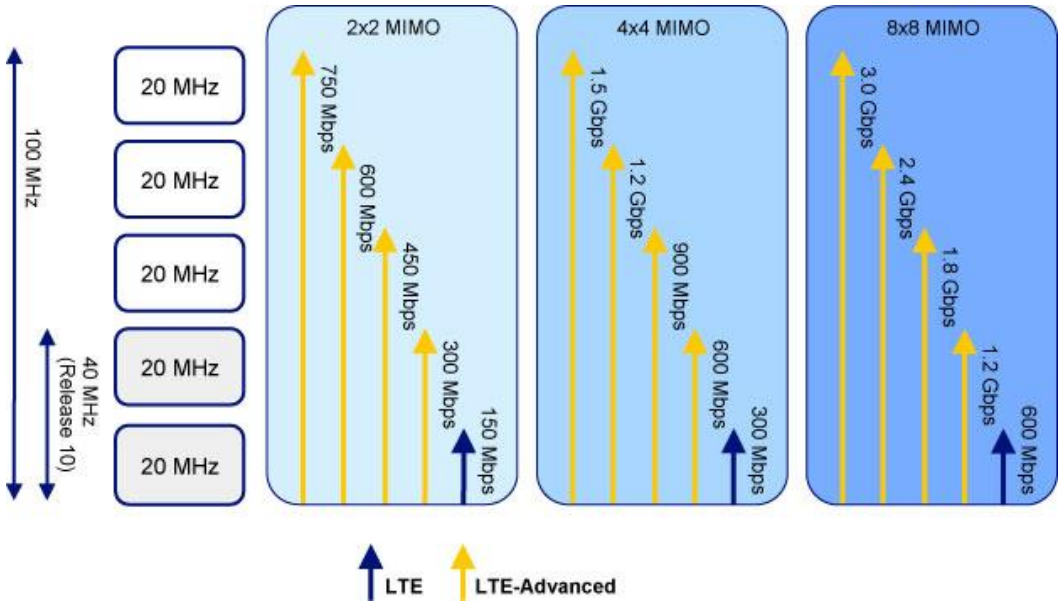


Figure 4. The available theoretical data transfer rates on LTE-Advanced [10].

As noted above the frequency spectrum is the pillar of wireless technologies. As expected, a much higher range will be allotted for the 5G than for existing mobile technologies. Currently the highest frequency band that used for mobile service in Hungary is the 2 600 MHz. The primary frequency band of 5G is currently set at around 6 GHz, which means an unusual high band in terms of radio service, but it is assumed that (after the disconnection of terrestrial broadcasting) the 700 MHz band could also be used in order to enable the nationwide and indoor 5G coverage [13].

The spread of radio signals weakens with increasing frequency and radio signals penetrates with more attenuation through materials and objects in the higher frequency range [14]. In the 6 GHz range the radio signal propagates with a level of degradation that it might require a denser network (an increase in the number of base stations) in order to supply nation-wide coverage. This could mean the largest investment that mobile operators have ever made regarding the access, the transmission and the core networks. The transmission network will most likely be a system of optical networks or possibly in the future of high-performance microwave devices [15]. The expected frequency bands for the 5G are shown in Fig. 5.

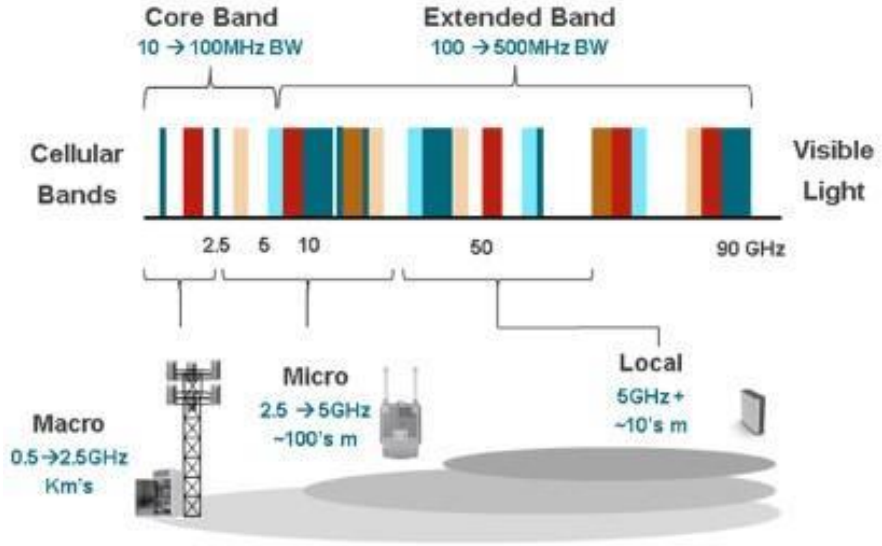


Figure 5. The planned band and the use of frequency ranges of the 5G [16].

In exchange the 5G will provide the highest data transfer rate that has ever been experienced on mobile networks: it will offer near real time communication sans delay and also increased capacity. The data transfer rate is expected to be 10 to 20 Gbps for one subscriber, the delay of the network might be less than 1 ms and the capacity could be ~1000 times more than that of existing technologies. As mentioned above, a denser network will be required, which means the number of users (that are in one cell) will decrease and this will also increase the capacity compared to previous technologies [17].

In Fig. 6 one can see the comparison of data transfer rate regarding the existing mobile technologies and the 5G.

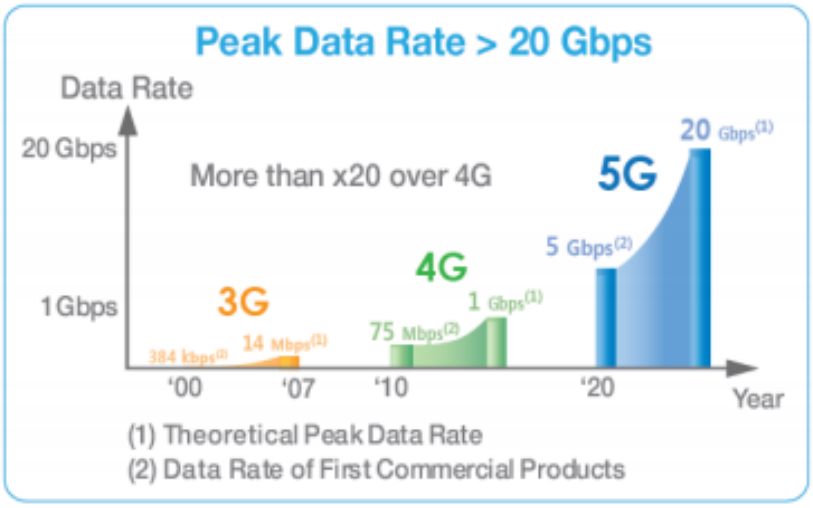


Figure 6. Representation of "Peak data rate" for 3G, 4G and 5G [18].

The real time latency can be a milestone in several sectors, such as healthcare or self-driving cars. Regarding medical surgeries the vision of 5G can be illustrated with the following examples. As the 5G will offer high data transfer rate and almost zero network latency, the surgical interventions could be made remotely – even from a continental distance – without a personal presence. With the help of high performance sensors (on the doctor's side) and robotic arms (on the patient's side), the surgery can be performed in real time (due to approximately zero latency). After the release of self-driving automatic cars 5G could provide innovative solutions like avoiding traffic jams and accidents by connecting and synchronizing vehicles to each other. Each necessary manoeuvre (that will handled by automatic cars) could be realized immediately in real time [19].

In addition to the above the engineers, who are currently working on the 5G standard, are trying to reduce the complexity of the network compared to the 4G. The focus is on the environmental sustainability as well: the battery of a 5G device can be expected to use a hundredth of the energy required in case of a 4G terminal [18].

The 5G is also expected to serve machines rather than people directly, like IoT (Internet of Things), which means the connection between devices and the internet that will communicate in real time with each other. The number of these devices is expected to rise in the tens of billions by 2020 [19].

TRAFFIC FORECASTS

The swift evolution of mobile technology brings up the question, whether LTE-Advanced and 5G will be able to provide the high data transfer rate and capacity foreshadowed by the increasing number of users and data traffic trends. In order to find the answer, forecasts –

published by the Cisco – have been analysed, which might provide an insight for the growth of mobile data traffic and trends that are to be experienced in the coming years. In order to have an accurate result, a live network of a mobile operator has also been examined in this regard and will be discussed in the following section.

DATA TRAFFIC FORECASTS BY CISCO

There are some important milestones we might start with, which are also anticipated by Cisco's study. Over the past 5 years the global mobile data traffic has grown 18-fold.

- In the next 5 years the global mobile data traffic will reach a new milestone: The 4G networks will handle more than three-quarters of the global total mobile traffic by 2021;
- 4G connection will generate double traffic on average as a 3G connection;
- By 2021 the 5G will be 0,2 % of connections and 1,5 % of total traffic but a 5G connection will generate 4,7 times more traffic than the average 4G connection due to the high speed that the 5G is expected to provide [20].

The global mobile data traffic grew 63 % in 2016, which was a huge increase. The following figure shows how the data traffic in each region increased in 2016. Central and Eastern Europe saw a 64 % increase, while data traffic in Western Europe grew by 52 %.

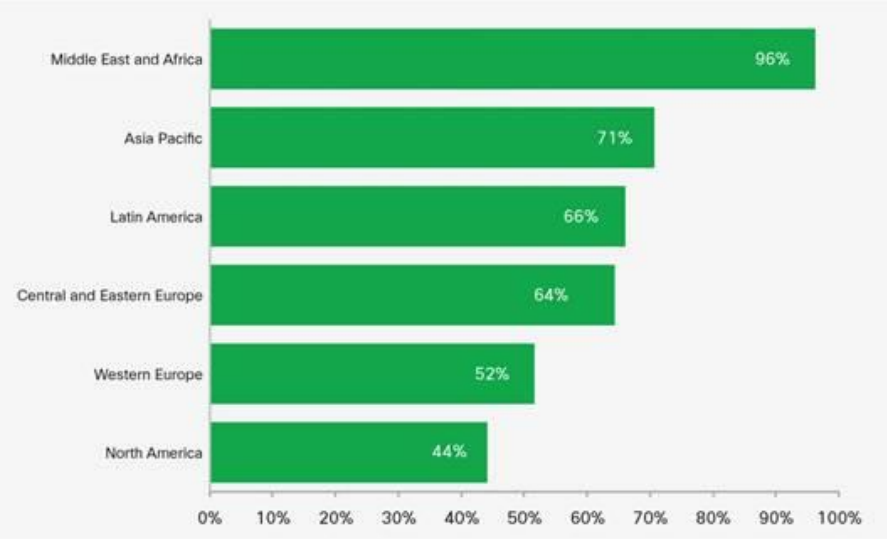


Figure 7. Mobile Data Traffic Growth in 2016 [20].

By 2021 the overall global mobile data traffic is expected to grow to 49 Exabytes per month, which means a seven-fold increase from 2016 to 2021. During this period the mobile data traffic will grow at CAGR (Compound Annual Growth Rate) of 47 %. Expectations of the coming years are shown on the next figure [20].

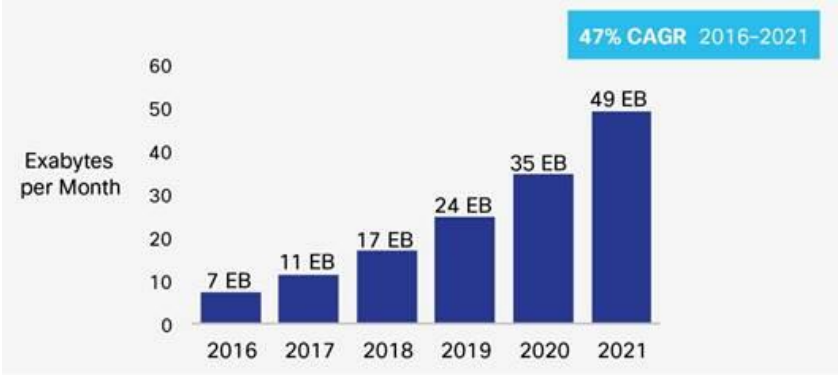


Figure 8. Cisco Forecasts 49 Exabytes per Month of Mobile Data Traffic by 2021 [20].

Cisco also predicts that 4G networks will become increasingly dominant by 2021, 56 % of the terminals will already be driven on 4G networks, but 3G networks will also have a minimal 2 % increase. However the proportion of 2G (GSM) usage will decrease from 42 % to 11 % between 2016 and 2021. The reason for this is that the ratio of devices capable only of 2G will decrease, therefore the 2G is not expected to follow an increasing trend. The newest technology, the 5G will produce more than 1000 % rise regarding the number of connections (2,2 million in 2020 to over 24,5 million in 2021), which ratio includes M2M (Machine to Machine) connections as well, as illustrated in Figure 9 [20].

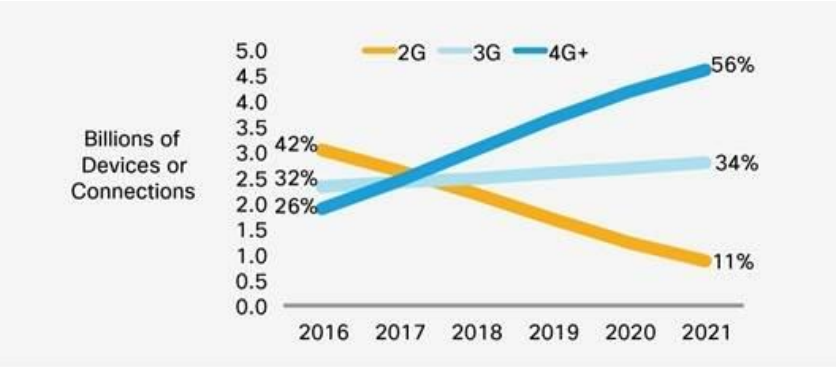


Figure 9. Global Mobile Devices (Excluding M2M) by 2G, 3G, and 4G+ [20].

4G carried 69 % of total global mobile traffic in 2016 by representing the largest share of mobile data traffic by network type. It will grow exponentially faster than other technologies to represent 79 % of all global mobile data traffic by 2021. 5G will support 4G with 1,5 % of mobile traffic by 2021 and provide high bandwidth (1000 Mbps) and ultra low latency (1 ms) [19, 20].

A 4G connection currently generates nearly four times more traffic than a 3G connection. 4G networks provides significantly more data traffic rates and drive users with greater bandwidth usage, thus the terminals on 4G are expected to generate much more traffic than on 3G. The following figure summarizes the mentioned prognosis and shows the ratio of overall data traffic in exabytes per month [20].

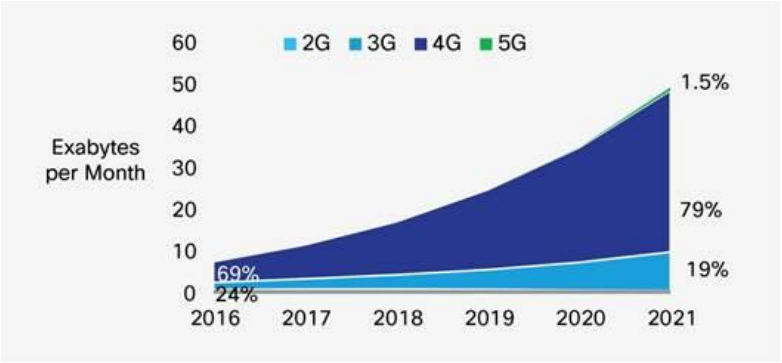


Figure 10. Global Mobile Traffic by Connection Type [20].

Cisco's research showed that the data traffic on mobile networks will nearly increase 1,5-fold per year [20]. Cisco has also made a study about the data transfer rates that will expected to be available on average by 2021, as shown in Fig.11.

The 4G data transfer rate will nearly double by 2021 according to Cisco, which can be realized for instance through carrier aggregation.

In order to handle the forecasted significant increase of data traffic in the next few years, it seems to be necessary to re-allocate new frequency bands (which were explained in the first chapter) in order to launch new 4G layers (use of the 4G on several frequency bands) and use LTE-Advanced.

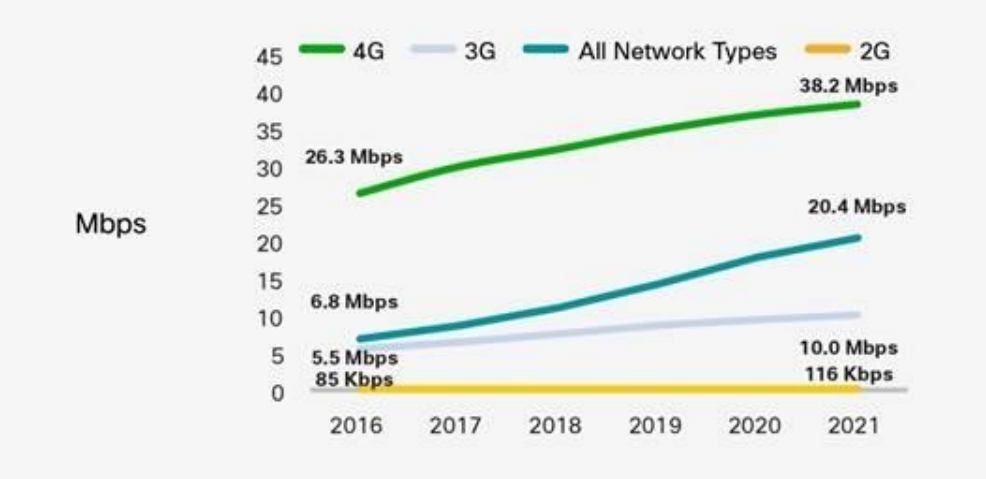


Figure 11. Mobile Speeds by Technology: 2G Versus 3G Versus 4G (Source: Cisco VNI Mobile, 2017; Ookla Speedtest.net) [20].

DATA TRAFFIC FORECAST REGARDING LIVE MOBILE NETWORK USAGE

As it has already been mentioned above, the operations of a mobile service provider have also been examined in respect of data traffic change. The operator has more than 5 million subscribers. Trends of data traffic were analysed using data collected from three mass events and three large cities.

Changes in Data Traffic of Mass Events

For major events, the mobile operators install temporary base stations to ensure high data transfer rate, capacity and quality in order to provide great customer experience and uninterrupted service. Regarding temporarily installed mobile networks of mass events (like a festival attracting tens of thousands of users) it can be said that they have the required capacity as it could be able to meet the demands of a whole town or a large city. Thus the annual data traffic of these events might provide a good prognosis for the annual increase of live mobile network on average, and also could provide a feedback to Cisco's forecast.

The events that were analysed had 45k-100k visitors, who were present at the same time. As there are a plenty of user located in a small area, this means a challenge from mobile operator point of view to deal with the demand in proper quality and without any interruption of service. For the analysis broadband mobile networks (3G, 4G) are in the focus. The 2G network was not analysed, because the data traffic – driven by the 2G network – is negligible compared to broadband networks.

Event 1 lasted 5 days on a territory of about 0,12 km^2 and had 45 000 visitors (who were present at the same time). Fig. 12 shows the increase in data traffic. The diagram starts in 2015 and the comparison expands to the following two years, the growth is presented in percentage. The table contains upload and download data aggregated and show the change of 3G and 4G network traffic separately and cumulatively as well.

Event 2 was bigger than Event 1 regarding its geographical size (~0,17 km^2), the number of users and the mobile network. ~50 000 people stayed at the same time on the 4 days long event. Fig. 13 shows the result of the last three years.

Event 3 was located on a ~1 km^2 territory and counts 100 000 people at the same time, lasted for 7 days and proved to be the most demanding from a mobile network capacity point of view. Its data traffic change is presented in Fig. 14.

The total data traffic – on 3G and 4G overall – grew to 1,9-fold at Event 1 from 2015 to 2016 and doubled from 2016 to 2017. This load mostly affected the 4G network. The data traffic of 3G network had a downturn in 2016 compared to 2015 and increased a bit in 2017 compared to 2016 (the load of 2017 exceeded the amount of data traffic – experienced in 2015). The 4G network usage grew more than 2.8-fold from 2015 to 2016 and it doubled from 2016 to 2017.

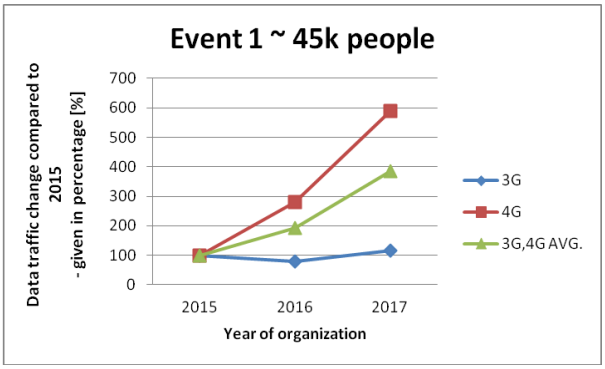


Figure 12. Data traffic change of Event 1.

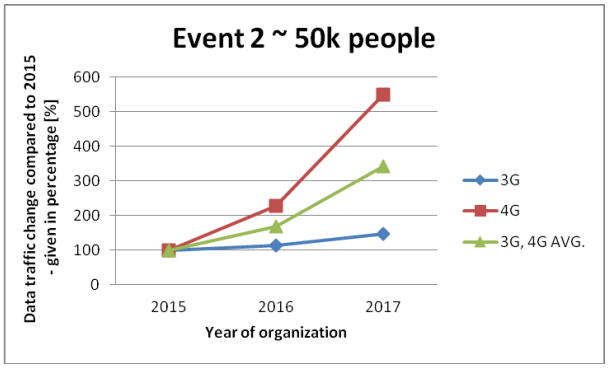


Figure 13. Data traffic change of Event 2.

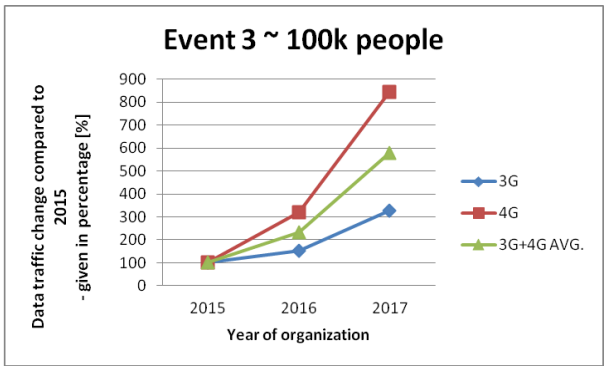


Figure 14. Data traffic change of Event 3.

The data traffic of Event 2 – similar to Event 1 – grew to about 1,7-fold from 2015 to 2016 and doubled from 2016 to 2017. 3G traffic saw a minor increase, while 4G traffic increased considerably.

The traffic of Event 3 doubled from 2015 to 2016 and it nearly grew to 2,5-fold by 2017 including 3G and 4G data. 2,3-times more data was driven through the 4G network in 2016 than in 2015 and from 2016 to 2017 the traffic grew 2,6-fold.

According to Fig. 15, one can conclude that the more users were attending the events, the larger annual traffic growth was experienced. The data of analysed events shows an annual doubling in the volume of data at least.

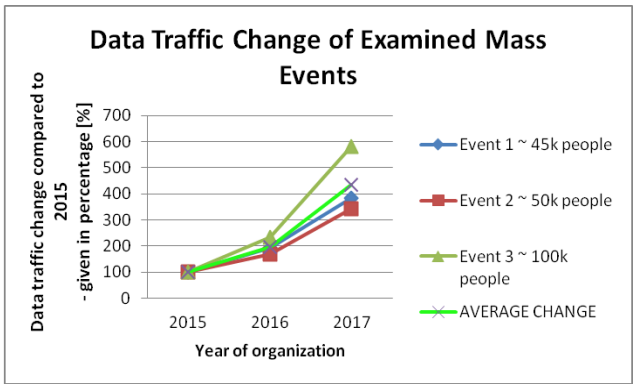


Figure 15. Data traffic change of analysed mass events – 2016, 2017 compared to 2015 (growth is given in percentage).

As stated previously – an intense increase could be discerned on the 4G network and minimal increase or lower decrease on the 3G network in 2016 and 2017 compared to 2015. The penetration of 4G terminals is rising year by year, the number of only 3G capable phones is decreasing, that is why there is more data going through 4G network broadband mobile networks.

Changes in Data Traffic of Large Cities

Three large cities – City 1, City 2 and City 3 were also examined in terms of data distribution. The sampling took place in September and was also analysed in 2016 and 2017.

City 1's geographical size is 280,8 km^2, the population is around 164 000. Fig. 16 shows the data traffic in September of City 1 regarding the last two years (growth is given in percentage). City 2 is located on 461,2 km^2 territory with a population of 204 000. Fig. 17 shows the result of the sampling months. City 3 (territory: 525,2 km^2), with a population of 1732 000 people, was also examined, and the data obtained is shown in Fig. 18.

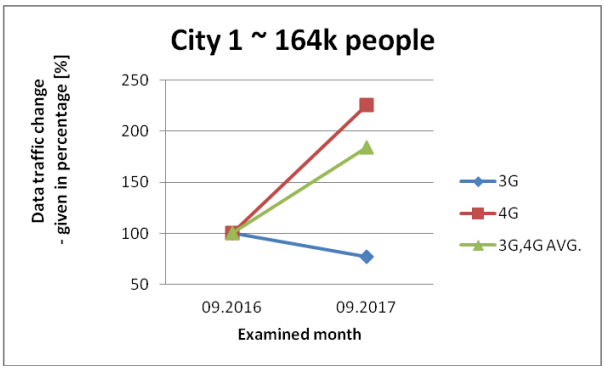


Figure 16. Data traffic change of City 1.

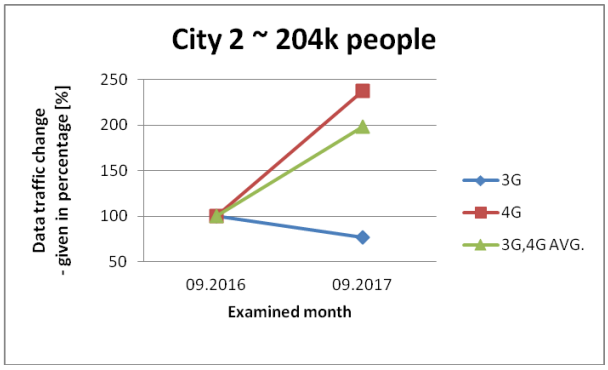


Figure 17. Data traffic change of City 2.

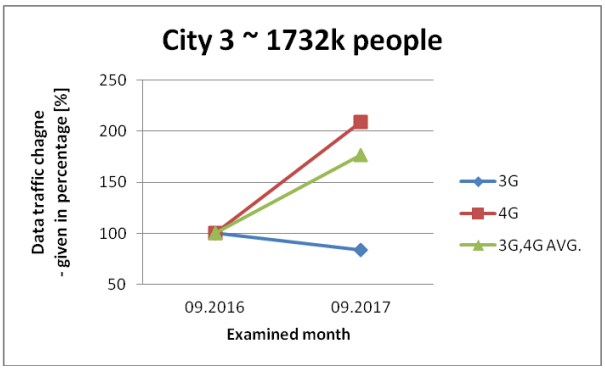


Figure 18. Data traffic change of City 3.

The data traffic usage of City 1 grew by 1,8-fold compared the data of September 2016 to the same month in 2017. The use of 3G data declined by 20 %, while the use of the 4G network significantly increased. The dataflow on 4G was more than 2,2 times higher in September 2017 than a year earlier.

Data traffic of City 2 also shows an increase in 2017, almost 2 times higher traffic was handled in 2017 than in 2016. This was achieved by the decline of 3G traffic by more than 23 %, while the 4G network generated nearly 2,5 times increase in September 2017.

The data volume of City 3 grew by nearly 80 % in September 2017 compared with the same month of 2016. The data usage decreased more than 16 % on 3G, so the 4G network had more than twice as much traffic in 2017. The increase in data traffic of large cities is summarized in Figure 19.

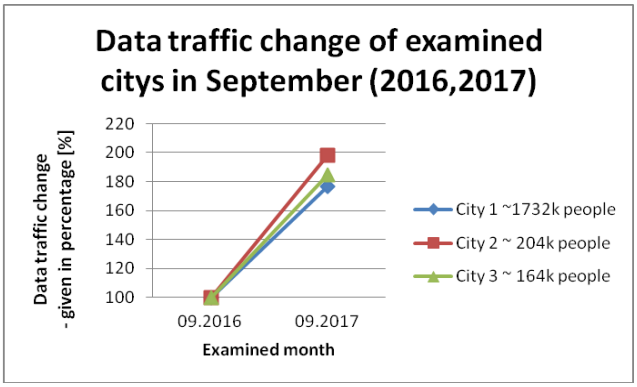


Figure 19. Data traffic change of the largest cities September 2016 compared to September 2017.

Based on live network results it can be noticed that concerning large cities the annual traffic was about 80 % more in September 2017 than in September 2016. The most densely populated city saw a more minor, but also significant increase in data traffic.

CONCLUSIONS

The results in the previous chapters show a major increase in data traffic both in the Cisco forecasts and in the live network analysis. According to Cisco and live mobile network data we can say that the data traffic on mobile networks is close to doubling each year. At the events that were under review, the utilization of 3G networks grew slightly and decreased only in one case in the examined years, while 3G traffic – in the cities that were surveyed – recorded a remarkable decline in the sampled month. On the 4G network there was a considerable and unstoppable increase experienced on mass events and in large cities as well. The results of live network analysis are in line with Cisco's forecast considering aggregated data traffic and shows disparity in the case 3G network usages. A possible explanation for

this might be that the penetration of 4G capable terminals seemed greater in large cities, therefore the 3G took a back seat.

All this leads to the conclusion that mobile operators have a tough task due to the significant data traffic growth. Now we may answer the question posed in the abstract of this article: The LTE-Advanced and the upcoming 5G (that is still under standardization) is capable of a very high speed, but is this rapid innovation, high data rate and huge capacity really necessary? The answer is clear on the basis of the results: yes.

The new technologies (like the 5G) and features could provide a tool for the service providers to increase the available data transfer rate, which is important from a capacity point of view as well: the higher the available data rate, the faster the mobile user downloads the data and for the shorter time the network resources are utilized (the data transfer rate has an indirect effect on the capacity).

Based on the results of live mobile networks and Cisco, the service operators might have to invest into cutting-edge technologies and features in order to keep up with the trends of growing traffic, thus there is a need for launching new 4G layers and using LTE-Advance until the arrival of the 5G. It is already apparent that in the upcoming years the implementation of new technologies (such as the 5G) will be essential in order to handle the forecasted traffic increase in sufficient quality and without congestion and interruption. 5G is the key technology for smart cities [21].

REFERENCES

[1] Ghasemi, Z.A.; Abedi, A. and Ghasemi, F.: *Propagation Engineering in Radio Links Design*. Springer Nature Switzerland AG., New York, pp.3-28, 2013, http://dx.doi.org/10.1007/978-1-4614-5314-7,

[2] NMHH: *Documentation for the tender announced in the announced in the subject of spectrum licences for broadband services*. NMHH, 14-21, 2014, http://nmhh.hu/dokumentum/163049/eloadas_frekvenciasavok_bemutatasa_20140429.pdf, accessed 15th November 2016,

[3] NMHH: *Selection of the winners of the tender procedure announced in the subject of spectrum licences for broadband services.* NMHH, 1-29, 2014, http://english.nmhh.hu/document/165104/uf_1579288_2014_en.pdf, accessed 15th November 2017,

[4] European Commission: *Report from the Commission to the European Parliament and the Council on the implementation of the Radio Spectrum Policy Programme.* https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:52014dc0228&from=en, accessed 15th November 2017,

[5] NMHH: *National Media and Infocommunications Authority Spectrum Strategy 2016-2020.* NMHH, pp.4-14, 2016, http://english.nmhh.hu/dokumentum/170996/rss_nmhh_2016_komm_fin.pdf, accessed 15th November 2017,

[6] Freeman, R.L.: *Radio System Design for Telecommunications*. John Wiley & Sons, Hoboken, pp.535-546, 2007,

[7] Mishra, A.R.: *Advanced Cellular Network Planning and Optimisation 2G/2.5G/3G. Evolution to 4G*. John Wiley & Sons Ltd., Chichester, pp.417-437, 2007,

[8] Singh, N.P.: *Theoretical and Real World of 4G*. International Journal of Mobile Network Design and Innovation **5**(2), 10-17, 2013, http://dx.doi.org/10.1504/IJMNDI.2013.060227,

[9] Xu, T. and Darqazeh, I.: *Bandwidth Compressed Carrier Aggregation.*
IEEE ICC 2015 – Workshop on 5G & Beyond – Enabling Technologies and Applications. IEEE, London, 2015,
http://dx.doi.org/10.1109/ICCW.2015.7247325,

[10] Hawke, D.: *5 Years to 5G: Enabling Rapid 5G System Development*.
EE|Times, 2015.
http://www.eetimes.com/author.asp?doc_id=1325670, accessed 29th December 2016,

[11] Hoydis, J.; ten Brink, S. and Debbah, M.: *Massive MIMO in the UL/DL of cellular networks: How many antennas do we need?*
IEEE Journal on Selected Areas in Communications **31**(2), 160-171, 2013,
http://dx.doi.org/10.1109/JSAC.2013.130205,

[12] Mitra, R.N. and Agrawal, D.P.: *5G mobile technology: A survey.*
ICT Express **1**(3), 132-135, 2015,

[13] European Commission: *Opinion on spectrum related aspects for next-generation wireless systems (5G).*
Radio Spectrum Policy Group, Brussels, pp.2-6, 2016,
http://rspg-spectrum.eu/wp-content/uploads/2013/05/RPSG16-032-Opinion_5G.pdf, accessed 15th November 2017,

[14] Durgin, G.; Rappaport, T.S. and Xu, H.: *Radio Path and Penetration Loss Measurements in and around Homes and Trees at 5,85 GHz*.
IEEE Antennas and Propagation Society International Symposium. IEEE, Atlanta, 1998,

[15] Fiorani, M., et al: *On the Design of 5G Transport Networks.*
Photonic Network Communications **30**(3), 403-415, 2015,
http://dx.doi.org/10.1007/s11107-015-0553-8,

[16] Artizanetwork: *DL/UL Acceleration Technologies, Artizanetwork*.
http://www.artizanetworks.com/lte_resources/lte_tut_adv_acceleration.html, accessed 25th November 2016,

[17] Yang, L. and Zhang, W.: *Interference Coordination for 5G Cellular Networks*.
Springer Cham, Heidelberg, 2015,
http://dx.doi.org/10.1007/978-3-319-24723-6,

[18] Arcep: *5G: Issues & Challenges*.
https://www.arcep.fr/uploads/tx_gspublication/Report-5G-issues-challenges-march2017.pdf, accessed 15th November 2017,

[19] Mavromoustakis, C.X.; Mastorakis, G. and Batalla, J.M.: *Internet of things (IoT) in 5G Mobile Technologies*.
Springer International Publishing, Heidelberg, 2016,
http://dx.doi.org/10.1007/978-3-319-30913-2,

[20] Cisco Visual Networking Index: *Global Mobile Data Traffic Forecast Update*.
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html, accessed 29th November 2016,

[21] Tokody, D. and Mezei, I.J.: *Creating smart, sustainable and safe cities.*
2017 IEEE 15th International Symposium on Intelligent Systems and Informatics. IEEE, Subotica, 2017,
http://dx.doi.org/10.1109/SISY.2017.8080541.

Interdisciplinary Description of Complex Systems 17(1-A), 40-50, 2019

PENSIONERS IN SMART CITY – THE MODELS OF THE SMART PENSION SYSTEM

Zsolt Szabó*

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

DOI: 10.7906/indecs.17.1.6
Regular article

Received: 26 March 2018.
Accepted: 31 December 2018.

ABSTRACT

The reform of the pension system is a cardinal and noteworthy subject in all countries of the European Union (EU), particularly the Visegrád Four. Visegrád Four are the four central European post-communist countries, the Czech Republic, the Republic of Hungary, the Republic of Poland and the Slovak Republic – the issue of ageing society and the problems of its pension systems' is often discussed in myriad scientific meetings. These economic and social challenges necessitate long-term government strategies, which need to be modelled, simulated (tested and verified). The study shows the numbers and the problems of the state pension system of Visegrád Four, particularly with regard to the main problems of Hungarian social security system is based on the expected population and demographic statistics. The study is based on statistical projections, it includes an attachment of the results of a questionnaire-based behavioural economics research, a presentation of a vision of pension expenses and pension standards in EU and Hungary.

KEYWORDS

modelling of the pension system, microsimulation, impact assessment of the pension system

CLASSIFICATION

JEL: I23, J61

*Corresponding author, η: zsolt@tamiyaryu.hu; +361 66 65 375;
DSSSS, Óbuda University, Bécsi út 96/b., H – 1034 Budapest, Hungary

INTRODUCTION: CHANGING OF THE POPULATIONS OF THE EUROPEAN UNION AND V4

At present most countries' social insurance systems are pay-as-you-go (PAYG) systems, i.e. expenses of pensions being payed are covered by the inpayment of jobholders [1]. The theoretical foundation of this kind of pension system was introduced in a publication of Paul Samuelson in 1958 [2]. This theoretical foundation is based on the presumption that the active members of a society support the elderly. This presumption is valid only if the number of babies being born is sufficient to insure enough active future jobholders to support the preceding generation(s). Another presumption of Samuelson is that as the population increases, the economy also grows [3].

We can examine the distribution of the population by age with a population pyramid. As the first figure shows, the calculations of the website https://populationpyramid.net show that the population of Europe is going to decrease. The figure represents the pyramid of ageing societies. According to precalculations, rapid ageing can be expected, which endangers the long-term sustainability of the pension systems of the European countries [4-7].

The population pyramid of Visegrád Four (V4), see Figs. 1-5, can be found on the website mentioned. According to the second figure, Hungary's population, similarly to the population of the European Union, is going to be stagnant in 2050.

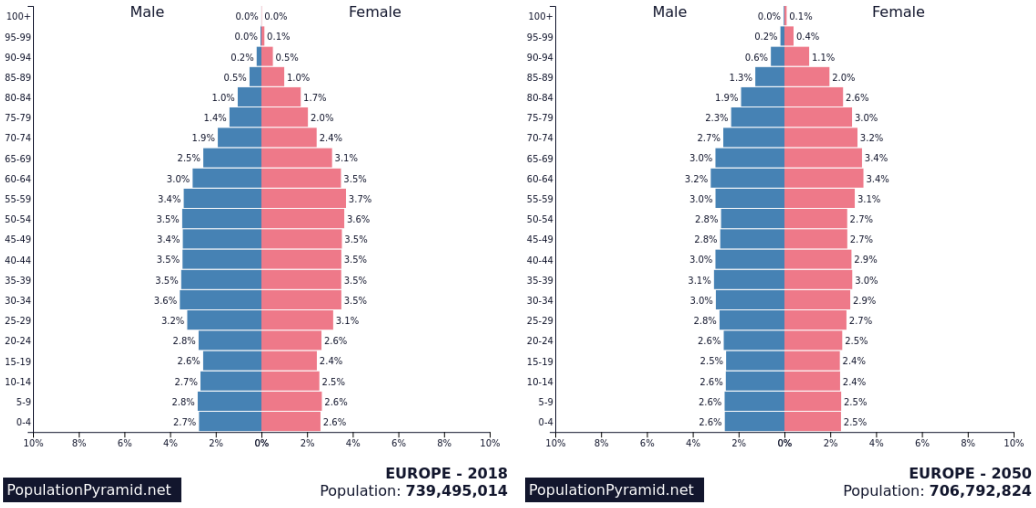


Figure 1. Population pyramid of Europe in 2018 and 2050.

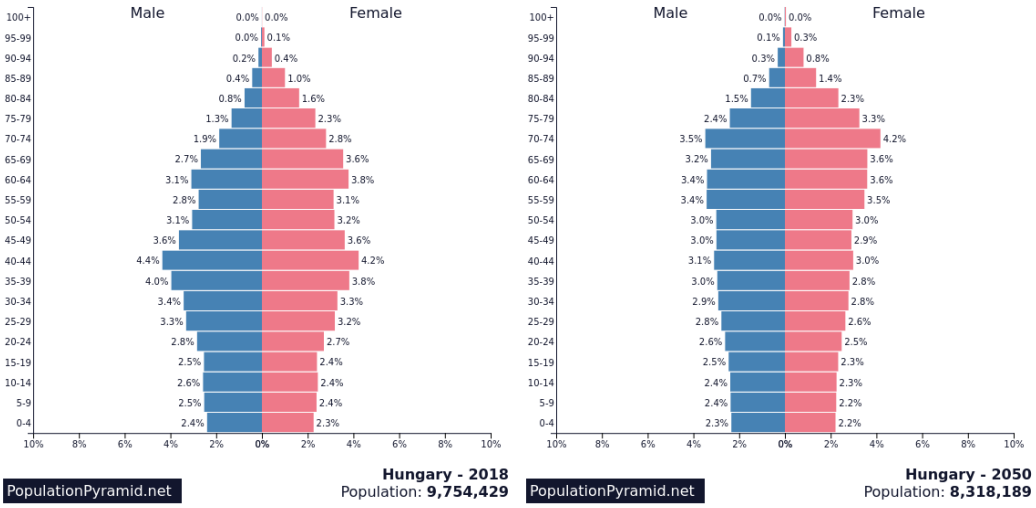


Figure 2. Population pyramid of Hungary in 2018 and 2050.

Fig 2 shows that in Hungary in 2050 the proportion of young and very old people is almost the same as in 2018, but between these two age ranges the pyramid is radically different, which will be the subject of further research.

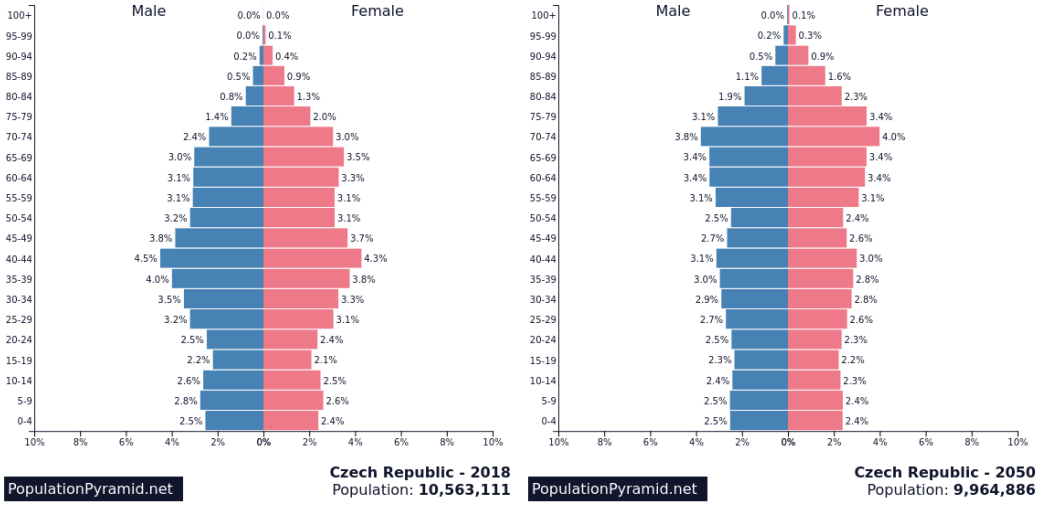


Figure 3. The population pyramid of the Czech Republic in 2018 and 2050.

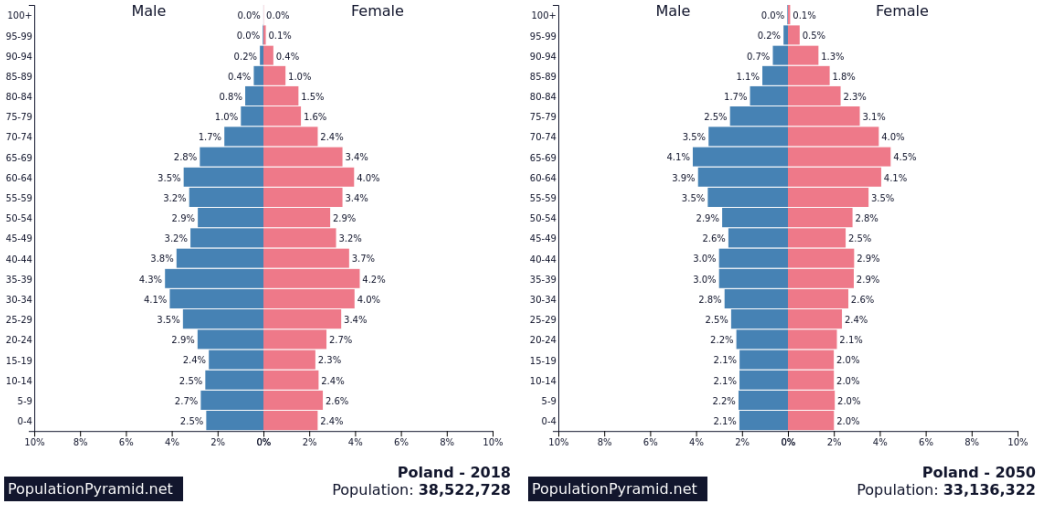


Figure 4. Population pyramid of Republic of Poland in 2018 and 2050.

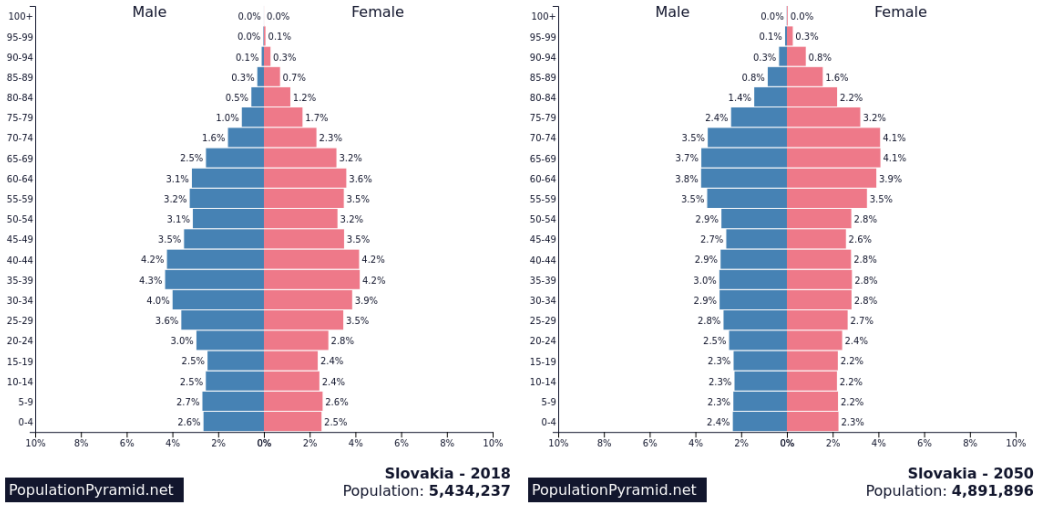


Figure 5. Population pyramid of Slovak Republic in 2018 and 2050.

Based on these reports, in Eastern Europe in the next few decades it is dramatically decreasing. Among the fastest shrinking ethnic groups in Eastern Europe (some in Central and Northern Europe) according to the UN 2017 forecasts [4]. According to Table 1, EU and V4, their population shrinks by 5 % or more. Hungary, Poland, their population shrinks by 15 %.

The tables show the precalculations of a study of the Commission of the European Parliament (EPC) [5-7]. According to the study, rapid ageing of the population of the European Union can be expected as a consequence of the growing life expectancy of men and women. Precalculations assume that the number of births is not going to change significantly (see Table 2).

Table 3 demonstrates the dramatic changes in the number of job-holders: the active part of the population is going to decrease radically. The size of the active population (working-age population aged 15-64 years) will be greatly reduced, which is expected to lead to a reduction in tax payments. On the other hand, pension expenditures are expected to grow in the EU Member States.

Table 4 shows that the ratio of pensioners and working-age people in EU and V4 are likely to grow at the same time.

Table 1. Current and future population of EU and V4 [4].

	2018, million	**2050, million**	**change, %**
European Union	739,49	706,79	-5
Hungary	9,72	8,28	-15
Slovak Republic	5,43	4,89	-10
Poland	38,17	32,39	-15
Czech Republic	10,56	9,964	-6

Table 2. Fertility rate for EU and V4 [5].

	2016	**2020**	**2030**	**2040**	**2050**	**2060**	**2070**
European Union	1,55	1,61	1,67	1,71	1,74	1,77	1,80
Hungary	1,48	1,61	1,68	1,72	1,75	1,77	1,80
Slovak Republic	1,40	1,47	1,60	1,68	1,74	1,79	1,82
Poland	1,37	1,45	1,56	1,61	1,65	1,68	1,71
Czech Republic	1,62	1,68	1,74	1,76	1,78	1,80	1,82

Table 3. Working age population, age 15-64, as % of total population for EU and V4 [5].

	2016	**2020**	**2030**	**2040**	**2050**	**2060**	**2070**
European Union	65,3	64,1	60,9	57,9	56,1	55,7	55,9
Hungary	67,1	65,0	63,0	60,4	57,4	55,6	56,0
Slovak Republic	70,0	67,7	64,5	61,9	56,8	53,9	54,7
Poland	68,7	66,0	62,6	61,1	55,9	52,4	55,6
Czech Republic	65,9	63,7	62,5	60,3	55,7	54,5	57,0

Table 4. Ratio of pensioners and working-age people in EU and V4 [5].

	2016	**2020**	**2030**	**2040**	**2050**	**2060**	**2070**
European Union	29,9	32,5	40,3	48,0	52,3	53,1	52,2
Hungary	27,5	31,3	35,2	41,8	49,1	53,2	52,0
Slovak Republic	21,0	24,9	32,9	39,7	51,5	59,4	56,8
Poland	23,7	28,4	37,3	42,6	55,3	64,9	62,2
Czech Republic	28,1	31,9	36,2	42,6	52,2	55,7	49,7

In order for the PAYG pension system to be maintainable in a society, the number of jobholders needs to be significantly larger than the number of retired citizens – otherwise the system is going to become imbalanced. Table 4 shows the ratio of pensioners and working-

Table 5. Potential GDP (growth rate) for EU and HU [5].

	2016	2020	2030	2040	2050	2060	2070
European Union	1,3	1,4	1,2	1,2	1,4	1,5	1,4
Hungary	1,9	1,9	2,1	1,2	1,5	1,3	1,3
Slovak Republic	2,4	2,8	2,8	1,8	1,2	1,2	1,5
Poland	2,7	2,6	1,9	1,2	0,7	1,0	1,0
Czech Republic	2,2	1,9	1,8	1,1	1,1	1,5	1,4

age people. According to the precalculations of EPC, the proportion of younger and older people is not going to change in a positive direction as the population of the elderly is going to increase, while the young (working) population is going to decrease. The fifth table shows the change in GDP. As GDP is expected to fall in V4, funding for pensions will probably entail increasing burdens. Financing pension payments will likely become a heavier burden on countries of the European Union, including V4.

Figure 6 shows the microsimulation modelling of the population. A similar microsimulation model is used in Hungary to estimate the size of the population in the future. Specialized administrative and other organizations are conducting more and more research into how the size of the population will affect macro- and micro-economical processes and the sustainability of the state pension system in the future.

PENSION MODELLING IN EU AND V4

State pension systems are targeting long-term goals and have long-term impacts. [1]. The Hungarian pension system is founded on two main pillars: the first pillar is the PAYG principle, the second is the capital provision principle [12]. In the case of a pension system based on the PAYG principle, the incoming contributions are not capitalized nor invested, but pensions are payed directly from them. The PAYG system is comfortable and might seem attractive while the population and the economy are growing. The recent obligatory social insurance system faces the following three problems that endanger the financial balance of the Hungarian pension system: an ageing population, a low level of employment and the partial payment of contributions. According to demographical data, the population stopped growing a long time ago. Meanwhile, pension payments are continuously growing as statistics show [8]. The PAYG system is undergoing a serious crisis in the European Union and the reforms of pension systems are inescapable. On a macro level an automatic system should be designed for contributions and pension payments that would ensure the long-term balance of the system [9].

A method to simulate the aforementioned problems and pension models with computers is microsimulation. This way there is no need for authoritative decisions – the effects of decisions can be simulated and calculated before the decision is made. The term “micro-simulation” is short for the expression “micro-analytical simulation” [5, 6, 11, 13, 14].

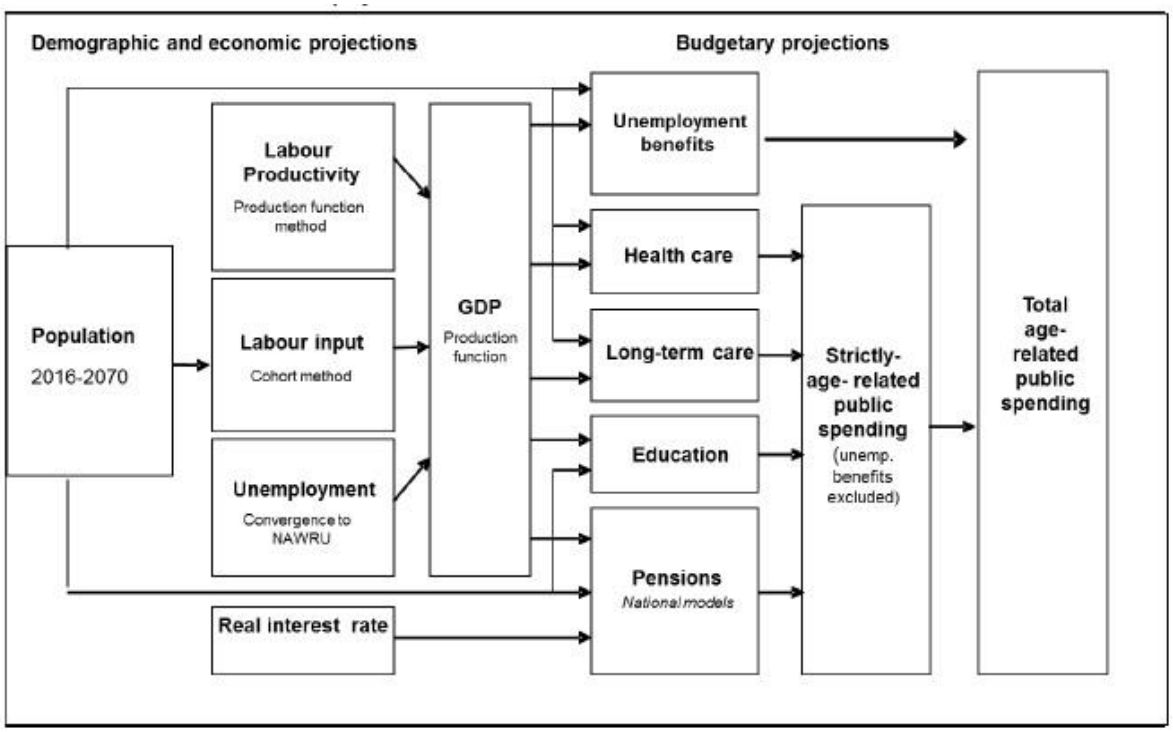


Figure 6. The microsimulation modelling process [5].

Table 6. Tools of modelling pension systems in EU and V4 [8].

Country	Financing	Public pension schemes	Model	Institution
Belgium	PAYG	DB	MIDAS-BE	Belgian Federal Planning Bureau (FPB)
Germany	PAYG	PS	AVID	Ministry of Labour and Social Affaires and the German Pension Insurance (MLSAGPI)
Sweden	PAYG	NDC	SESIM2	Ministry of Health and Social Affairs (MHSA)
Hungary	PAYG	DB	MIDAS-HU	Central Administration of the National Pension Insurance (CANPI)
Slovak Republic	PAYG	PS	IER	Institute for Economic Research (IER)
Poland	PAYG	NDC	ZUS	Polish Social Insurance Institution (PSII)
Czech Republic	PAYG	DB	NEMO	Ministry of Labour and Social Affairs (MLSA)

Micro-simulation models applied in the impact analysis of the pension system may be classified according to many aspects, from absolutely static to fully dynamic [8]. Micro-simulation modelling takes place at the level of individuals and households, i.e. in those locations where the direct impacts of the changes of the pension system are registered (see Fig. 6.). This way the changes in the distribution of various incomes (wages, pensions) in time can be modelled Pension systems are for the long term and therefore they have long-term impacts. According to demographic figures, the population has not grown for a long time, and preliminary calculations show that the growth of the economy has stalled and pension expenditures keep increasing [5-9]. Recently, PAYG systems are in a deep crisis

everywhere in the world, therefore the reform of the state-operated pension system has become inevitable. It is essential to assess the impacts of actions, and micro-simulation is an excellent method for this. The task of pension calculation requires the long-term forecast of data and that can be done through modelling (in the U.S. calculations are performed for 75 years, in the EU and in V4 for 50 to 60 years ahead) [8]. In general, we use the following micro-simulation models in the impact analysis of pension systems (see Table 6.) [15]. Dynamic simulation is generally used, where the demographic modules also have to be created. In Hungary the predicted number of births, deaths, marriages and divorces necessary for the modules can be obtained from the statistical service of the state (KSH). Table 6. shows that countries of the EU use different tools for modelling their pension systems. Nowadays dynamic microsimulation models are used in public or semi-public research agencies or ministries in EU member states for policy assessment. Many models form the basis of international scientific publications and are therefore better known. Models developed in public institutions are less extensively documented (in English) and appear less often in international publications.

RESULTS: THE EXAMINATION OF SUSTAINABILITY

Microsimulation can predict the effects of planned measures therefore it can effectively help decision-making. Information is important for an economic entity, be it a state or private organization. Without information there is no progress, no possibility for planning, which results in fall-back and regression [16]. Safety and security are essential elements of the operation of an organization. The financing method of the pension systems (e.g. DB – defined benefit, PS – points, NDC – national accounts) also differ across countries (see Table 6.). While occupational and private pension schemes are usually funded, the degree of their funding relative to the pension promises may differ, due to the fact that future pension benefits can be related either to the salary and career length (defined-benefit system) or to paid contributions (defined-contribution system). Most public pension schemes are financed on a PAYG basis, whereby contribution revenues are used for the payments of current pensions. In most countries, minimum guarantee pensions are covered by general taxes. Earnings-related schemes are often subsidised to varying degrees from general government funds. Some specific schemes, notably public sector employees' pensions sometime do not constitute a well identified pension scheme but, instead, disbursements for pensions appear directly as expenditure in the government budget. On the other hand, some predominantly PAYG pension schemes have statutory requirements for partial pre-funding and, in view of the increasing pension expenditure, many governments have started to collect reserve funds for their public pension schemes. The actual PAYG pension system is still quite popular although it is going to face a serious crisis, therefore it will probably continuing a changed form. Experts suggest a mixed pension system (state pension and self-care forms together) but there is still no model everyone would accept as ideal. Now the sustainability of the state PAYG system will be examined in more detail according to a simplified mathematical model, based on macro and microeconomic aspects [11]. Based on economic activity, human life can be formally divided into three sections: childhood, active age and old age. In the first and third sections people do not do any paid work; in the second section they usually do [1]. At present the social insurance system is PAYG, that is, every year it is mostly the contributions of the workers that covers pension payments [3]. The simplified mathematical model of the PAYG system is the following [11, 16, 17]: Number of contribution payers × Pension contribution rate × Yearly average salary × Number of pensioners × Annual average pension. Table 5. shows that the number of people in paid employment is going to decrease, while the old-age dependency ratio is going to increase, therefore according to the formula the pension

contribution rate will have to be increased to keep the balance. Employees will have to pay more tax and contributions. Fig. 6. shows that in modelling usually the average salary and the average pension can be used, but it is important to take into account that everybody has a different career, salary and pension, if we wish to make actual calculations. In modelling usually the average salary and the average pension can be used, but it is important to take into account that everybody has a different career, salary and pension, if we wish to make actual calculations. When examining the sustainability of the state pension system, we have to examine the above-mentioned simplified mathematical model of the PAYG system. The number of pensioners is forecasted to increase drastically; this cannot be changed. This way the right side of the equation will increase and the balance will be upset. The question is how the balance can be reset. An increase in the number of people paying pension contributions: according to demographic forecasts, this number will not change considerably; what's more, it is likely to decrease. A solution can be to motivate young people to have more children. Increasing the pension contribution rate would mean a further tax burden on employers and employees. Increasing the yearly average salary: it cannot be increased very much because productivity is not high in Hungary. Decreasing the yearly average pension: pensions are low as they are, and further decrease would cost the ruling party many votes. Another possibility is raising the age of pension eligibility, which was suggested and introduced in many European countries. Wherever we make modifications in the formula, the system becomes imbalanced. The two sides should be macro-economically balanced. Therefore experts suggest the mixed system (public and private). In the current pension system, a supplementary element can be a voluntary pension fund. This may mean that the standard of living we got used to in our active years can be maintained after retirement. There exist other pension saving systems as well, such as pension insurance.

The research focused on the present and future state of the respondents. We wanted to know what customs and processes motivated them to choose the form of self-care, the pension system they chose. We examined the respondents with behavioural economics and factor analysis [18]. The starting point of the research project is that people think of pension with fear and uncertainty. Based on the previous chapters, it can be seen that the pay-as-you-go system is in a crisis, therefore the second pillar of the pension system, self-care, receives more and more attention. To understand the motivations behind the decisions of the respondents, we used factor analysis, which is a widespread method nowadays to map personality [19]. We processed the data of the surveys and carried out the statistical calculations with the SPSS software [20, 21]. The online survey was completed in 2017. The respondents were answering online on kerdoivem.hu (http://www.kerdoivem.hu/kerdoiv/927511662). The number of respondents was 500 altogether (n = 500). My basic questions were about pension systems, pension savings, self-care and retirement security because these determine the financial background of our future life, that is, the extent of our self-care. The replies were divided into three groups: 1) knowledge of pension systems (mandatory, voluntary), 2) financial planning (characteristics of various savings plans) and 3) the role of self-care (the mapping of personality). These three groups are analysed separately by the qualitative research. Several statistical characteristics were calculated, such as average and frequency, and we did cross tabulation analysis.

Table 7. shows further relationships, such as savings in the case of different ages. For example, people between 29-48 years of age consider savings important. Table 8. shows further relationships between pension savings and optimism. Pension savings are more important for optimist men than optimist women (shown by the higher number of 324 affirmative responses).

Table 7. The role of age in pension savings.

		Has pension savings?		Total
		Yes	No	
Age, years	between 15-19	1	63	64
	between 19-28	48	162	210
	between 29-48	100	73	173
	over 49	33	20	53
Total		182	318	500
Percentage, %		36,4	63,6	100

Table 8. The role of optimism in pension savings.

			Pension savings		Total
			Male	Female	
Optimist?	Yes	Number	324	12	336
		Percentage, %	96,4	3,6	100,0
		Pension savings %	67,4	63,2	67,2
		% Total	64,8	2,4	67,2
	No	Number	157	7	164
		Percentage	95,7	4,3	100,0
		Pension savings %	32,6	36,8	32,8
		% Total	31,4	1,4	32,8
Total		Number	481	19	500
		Percentage	96,2	3,8	100,0
		Pension savings %	100,0	100,0	100,0
		% Total	96,2	3,8	100,0

Young people think they have several options to make a foundation for their future financial situation. The state pension system is mandatory, however, as far as voluntary and private funds are concerned, our decisions are usually made according to our income and our emotional decisions. Generally speaking, respondents are most encouraged by the general economic situation and security at work, and the pension and health insurance systems in the future country.

CONCLUSION

According to forecasts, current pension systems are likely to cause severe social and economic problems globally because of the rapid ageing of our societies. Based on forecasts, the current pension regime, and the drastic change in the ratio between active wage earners and pensioners will, with a high degree of probability, cause social, economic and other problems in the future both globally and in our country. The issue of sustainability also highly affects the definition of the possible model. The wide range of tools of microsimulation can be used to model and plan the pension system. As we have presented in the study, using the tools of micro-simulation the concepts of the pension regime can be modelled quite well in advance; such modelling has become increasingly common and successful in the EU and also in V4. In our days planning a pension system requires the possession of skills and application of up-to-date planning methodologies. The sustainability of the PAYG pension system is determined by the ratio of the number of people in employment, or rather the number of people paying contributions and the number of pensioners, since pensioners get their pension from the contributions paid. Experts recommend a mixed pension system, in which self-care has an important role. The respondents think about many possibilities to supplement state pension. State pension is compulsory; therefore it has to be chosen. In the case of supplementary ways of self-care, the

choice of the form or forms of savings is determined by our income and emotional decisions. Of course, research cannot solve all the problems of the pension system but researchers can clearly define and examine possibilities and effective methods for prediction and problem-solving.

REFERENCES

[1] Augusztinovics, M. and Köllő, J.: *Decreased employment and pensions. The case of Hungary. Pension reform in Southeastern Europe. Linking to labor and financial market reform.* World Bank, Washington, 2009,

[2] Samuelson, P.A.: *An exact consumption-loan model of interest with or without the social contrivance of money.* Journal of Political Economy **66**, 467-482, 1958,

[3] Mészáros, J.: *Pension Adequacy and Sustainability.* Report. Conference of the Central Administration of National Pension Insurance. Ministry of Human Resources and the Ministry for National Economy. Budapest, 2013,

[4] United Nations: *World Population Prospects: The 2017 Revision*. United Nations, New York, 2018, https://esa.un.org/unpd/wpp/publications/Files/WPP2017_Volume-II-Demographic-Profiles.pdf, accessed 19th May 2018,

[5] European Commission: *Underlying Assumptions and Projection Methodologies.* The 2018 Ageing Report, 1-240, 2018, https://ec.europa.eu/info/sites/info/files/economy-finance/ip065_en.pdf, accessed 19th May 2018,

[6] European Commission: *The 2015 Ageing Report.* European Union, Brussels, 2018, http://ec.europa.eu/economy_finance/publications/european_economy/2015/pdf/ee3_en.pdf, accessed 19th May 2018,

[7] European Commission: *Pension Schemes and Pension Projections in the Eu-27 Member States 2008-2060.* http://ec.europa.eu/economy_finance/publications/pages/publication16036_en.pdf, accessed 19th May 2018,

[8] Central Administration of National Pension Insurance: *On using dynamic microsimulation models to assess the consequences hypotheses on pension adequacy: Simulation results for Belgium, Sweden and Hungary*. Federal Planning Bureau, Brussels 2015, https://lirias.kuleuven.be/bitstream/123456789/493177/5/rep_simubesehu0515_11026.pdf, accessed 19th May 2018,

[9] Dekkers, G.: *An introduction to MIDAS_BE, the dynamic microsimulation model for Belgium.* Working paper. Centre for Sociological Research, Brussels, 2013,

[10] Central Statistics Office: *Hungary 2015.* Central Statistics Office, Budapest, 2016,

[11] Simonovits, A.: *Modeling pension systems, Houndmills.* Palgrave Macmillan, Basingstoke, 2013,

[12] Novoszáth, P.*: Social security finances*. Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2014,

[13] Gilbert, N. and Troitzsch, K.: *Simulation for the Social Scientist*. Open University Press, Buckingham, 1999,

[14] Molnár, I.: *Statistical Review.* Statisztikai Szemle **82** (2004), 462-477, 2004,

[15] Gál, R.I.; Horváth, A.; Orbán, G. and Gijs, D.: *Monitoring pension developments through micro socioeconomic instruments based on individual data sources: feasibility study Final Report for The European Commission Employment, Social Affairs and Equal Opportunities DG EMPL E4 Unit.* TARKI Social Research Institute, 2018, http://ec.europa.eu/social/BlobServlet?docId=4300&langId=en, accessed 19th May 2018,

[16] Banyár, J.: *Model Options for Mandatory Old-Age Annuities*.
Gondolat Kiadó, Budapest, 2016,
[17] Szabó, Zs.: *The modelling and simulation of the pension system.*
IEEE 30th Jubilee Neumann Colloquium: Neumann Colloquium 2017. IEEE, Budapest, 2017,
[18] Varga, J. and Csiszárik-Kocsir, Á.: *Versenyképességi átrendeződés Közép-Kelet Európában, fókuszpontban a V4 országok, Kárpát-medencei versenyképesség.*
6. Báthory – Brassai Konferencia 2015. Óbuda University, Budapest, 2015,
[19] Szabó, Zs.: *Financial awareness of retirement savings: analysis of a survey in Hungary*.
Proceedings of the Symposium for Young Researchers FIKUSZ 2017. Óbuda University, Budapest, 2017,
[20] Sajtos, L. and Mitev, A.: *SPSS Research and Data Analysis Manual.*
Alinea Kiadó, Budapest, 2007,
[21] Petrovics, P.: *SPSS Tutorial & Exercise Book for Business Statistics*.
University of Miskolc, Miskolc, 2012.

Interdisciplinary Description of Complex Systems 17(1-A), 51-57, 2019

GLOBAL SOLAR ENERGY TRENDS AND POTENTIAL OF BUILDING SECTOR IN HUNGARY

Attila Talamon[1,]*, Roland V. Papp[1], István Vokony[2] and Bálint Hartmann[3]

[1]Szent István University, Institute of Architecture
Budapest, Hungary

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

[3]Centre for Energy Research, Hungarian Academy of Sciences
Budapest, Hungary

DOI: 10.7906/indecs.17.1.7
Regular article

Received: 20 May 2018.
Accepted: 31 December 2018.

ABSTRACT

As the present trends show current policies lay more stress on using solar energy and renewable energy sources as some years before. There is a 175 000 TW power of solar energy, which came from the Sun. If it could be exploited, less than 10 % of this would be enough to cover the human economy. The solar energy has an important role in the reduction of the Ecological Footprint of humanity. This research would be offered a survey the global solar energy trends and the potential of building sector in Hungary. Furthermore, also the alternative energy sources appeared in the transport: many governments give financial assistance to the proliferation of electric cars.

Government and policy support for renewable energy has increased considerably over the past decade. Two drivers underpin this trend: first, the effort to constrain growth in greenhouse-gas emissions and, second, concerns to diversify the supply mix (promoted particularly by high oil prices, especially in 2005-2008). To address these concerns, more and more governments are adopting targets and taking measures to enhance the share of renewables in the energy mix.

KEYWORDS

energy trends, solar energy, energy potential, building sector assessment, decision support

CLASSIFICATION

JEL: Q42

*Corresponding author, η: talamon.attila@gmail.com; +36 30 981 62 67;
Hungary, Budapest 1034 Bécsi út 100.

GENERAL GLOBAL ENERGY TRENDS

One of the major challenges faced by European countries today is the reduction of CO_2 emissions that contribute to climate change, and one of the key areas where improvements could be made easily and at low cost is the energy efficiency of buildings. There is an urgent need nowadays to reduce current levels of greenhouse gases emissions. Greenhouse Gases (GHGs) are water vapour (H_2O), carbon dioxide (CO_2), methane (CH4), nitrous oxide (N_2O), ozone (O_3), chlorofluorocarbons (CFCs) and hydrofluorocarbons (HCFCs, HFCs). On the other hand, the European Union (EU) countries are largely dependent on energy imports and vulnerable to disruption in energy supply, which may in turn threaten functioning of their current economic structure. The EU imported 54 % of its energy sources in 2006 and was projected to increase even further by 2030. Reducing its import dependency EU is one of the main goals of the 20-20 by 2020 target – this legislative package is believed to reduce the expected imports of energy by 26% compared to the development before the 20-20 initiative. There were three main directions of the 20-20 programme, which are the 20 % cutting of GHGs, the 20 % rising in the using of renewables and the development of energy efficiency by 20 %. The pledge of Hungary in this programme was the increasing of the renewable energy using with 14,65 % and the decrease of GHGs emission with 10 %. One of the most important environmental problems is the energy consumption of the buildings. It is shown in this paper that buildings can deliver large energy and CO_2 emission reductions at low costs. The directives and the methods of the energy certification of the buildings spread across Europe. Only 1-2 % part of the building stock is exchanged every year, so it is very important to increase the energy efficiency of the existing buildings, too.

As the statistics shows, in Middle Europe the gap to reach the 2020 renewable energy share target is on an average value. In Hungary the purposed value to 2020 is 14,7 % and the reached value in 2016 is 14,2 % [1]. In other Middle European countries, for example in Poland and in Slovakia the stance in 2016 was worse than in Hungary. The intent in Poland is 15,9 % and the reached value in 2016 was 11,3 %. The corresponding values in Slovakia in 2016 were 14,0 % to 12,0 %.

The following table shows the forecast in Poland. Accordingly, the three major energy user sectors in 2020 still the Industry, Households and Transport. This table is similar to other countries in this region, and based on this, it is clearly visible that the intervention may be the most efficient in these sectors.

Table 1. Demand for final energy by sectors of the economy in Poland, based on [2].

	2006	**2010**	**2015**	**2020**	
Industry	20,90	18,20	19,00	20,90	29 %
Transport	14,20	15,50	16,50	18,70	26 %
Agriculture	4,40	5,10	4,90	5,00	7 %
Services	6,70	6,60	7,70	8,80	12 %
Households	19,30	19,00	19,10	19,40	27 %
Total	65,50	64,00	67,20	72,80	100 %

Short-term changes in energy demand and the composition of the fuel mix are largely a function of economic conditions, energy prices and the weather. But long-term trends, as is shown by the strong contrasts across the main WEO-2015 (World Economic Outlook) scenarios, can be significantly changed by the manner in which governments intervene in markets to tackle energy-related challenges.

Nonetheless, several fundamental energy trends persist across the scenarios: rising incomes and population push energy needs higher; energy-market dynamics are increasingly determined by the emerging economies; fossil fuels meet most of the world's energy needs, from an ample resource base; and providing universal energy access to the world's poor remains an elusive goal [3] (Fig. 1.).

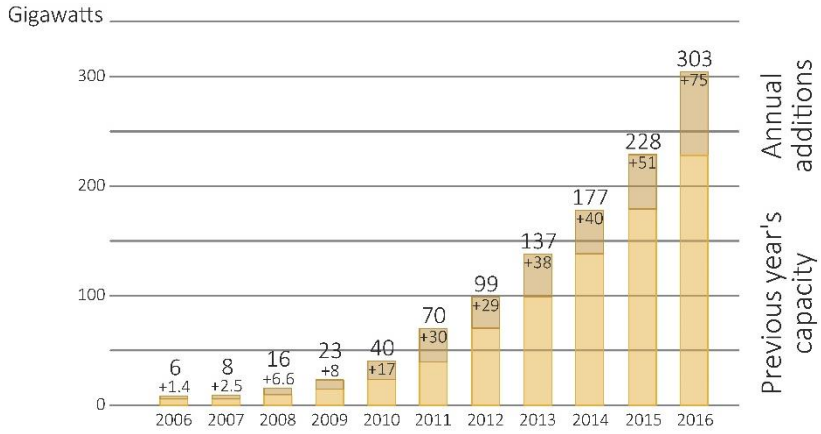


Figure 1. Solar PV Global Capacity and Annual Additions, 2006-2016, on the basis of [4].

RISING RENEWABLE ENERGY PARTICIPATION

In 2040, the share of renewables (including traditional biomass) in world primary energy demand could/would/planned to/etc. reach 15,7 %, from 12,6 % in 2010. This rapid increase is underpinned by incentives to overcome market barriers, falling technology costs, stronger application of policies, rising fossil fuel prices and in some cases carbon pricing (see Section 1). Most of the growth occurs in the power sector, where their share in total generation grows from 20 % to 31 %, a near tripling in actual generation.

Global demand for renewable energy continued to rise during 2011 and 2012, despite the international economic crisis, which makes us feel its influence in the future, on-going trade disputes, and policy uncertainty and declining support in some key markets. Renewable energy supplied an estimated 19,2 % of global final energy consumption by the end of 2014, the latest year for which data are available.

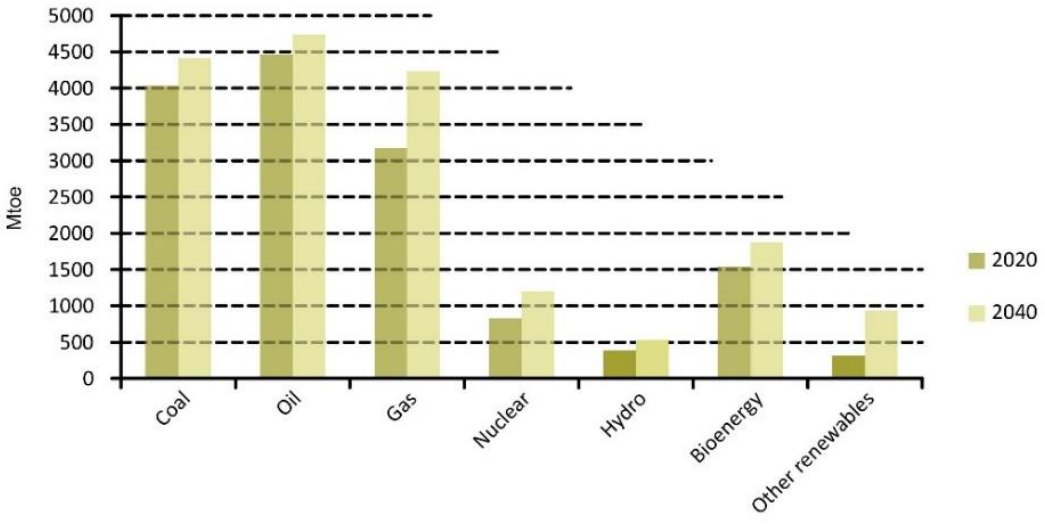


Figure 2. World primary energy demand by fuel in the New Policies Scenario, based on [3].

Of this total, approximately 8,9 % came from traditional biomass, which is used primarily for cooking and heating in rural areas of developing countries. Useful heat energy from modern renewable sources accounted for an estimated 4,2 % of total final energy use; hydropower made up about 3,9 %; and an estimated 1,4 % was provided by power from wind, solar, geothermal, and biomass and by biofuels. Among others this rate shows that the value of wind energy using is lower in 2014 than in 2012 (Fig. 2.).

Renewables are a vital part of the global energy mix. Modern renewable energy can substitute for fossil and nuclear fuels in four distinct markets: power generation, heating and cooling, transport fuels, and rural/off-grid energy services. This section provides an overview of recent market and industry developments in the first three sectors, while the Rural Renewable Energy section covers rural/off-grid energy in developing countries. The section that follows provides technology-specific coverage of market and industry developments and trends [5].

During the two-year period 2012-2014, installed capacity of many renewable energy technologies grew very rapidly, with the fastest growth in the power sector. Total capacity of solar Photo Voltaic (PV) grew at rates averaging 60 % annually. Concentrating Solar thermal Power (CSP) capacity increased more than 40 % per year on average, growing from a small base, and wind power increased 25 % annually over this period [5].

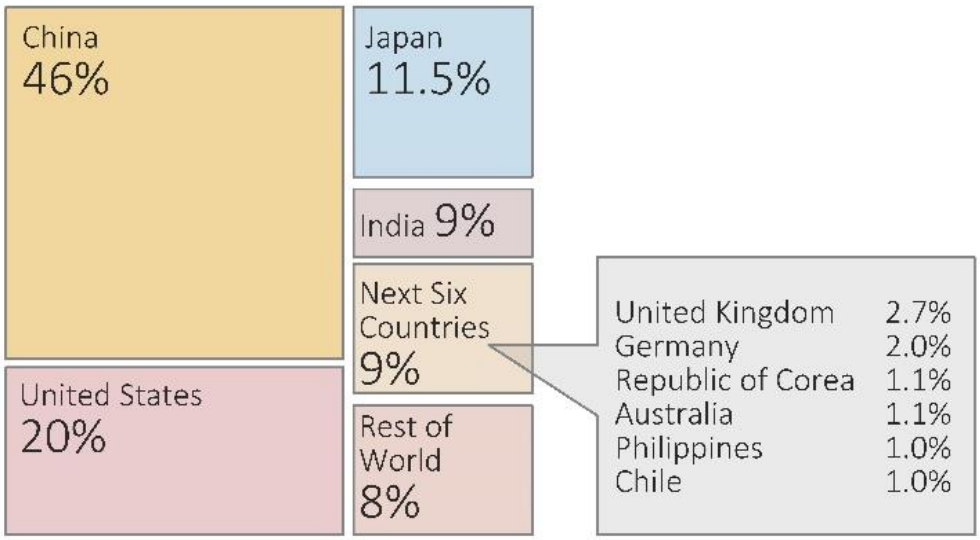


Figure 3. Renewable power capacities in the world, EU27, BRICS, and Top Seven Countries End-2015, based on [4].

PV additions shows us the fastest PV growing trends in the world. It shows that the leading country is China and the United States follows it with the half of its growing (Fig. 3.).

Hydropower and geothermal power are more mature technologies and their growth rates have been more modest, in the range of 3- 4% per year. Bio-power is also mature but with steady growth in solid and gaseous biomass capacity, increasing at an average 8 % annually. Demand has also increased rapidly in the heating/cooling sector, particularly for solar thermal systems, geothermal ground-source heat pumps, and some bioenergy fuels and systems [5].

RELEVANCE OF BUILDING SECTOR – ENERGY CONSUMPTION

Buildings are the largest consumers of energy. The sector's global final energy consumption doubled between 1971 and 2010 to reach 2 794 Mtoe, driven by population increase and economic growth. During current policies, global energy demand from buildings is projected to grow by an additional 838 Mtoe by 2035 compared to 2010 [6].

Most of this growth will result from the increase of building's energy use in non-IEA countries. The growing energy consumption of buildings is expected to effect heavy pressure on the global primary energy supply unless effective policy action is taken at a global level ((International Energy Agency) IEA, 1994).

In most EU member countries, buildings currently account for more than 40 % of primary energy consumption. [7] The residential sub-sector remains the largest consumer of energy at a global level, and the non-residential sub-sector has increased its share since 1990, especially in Brazil, Russia, India, China and South Africa (BRICS) [8] (Fig. 4.).

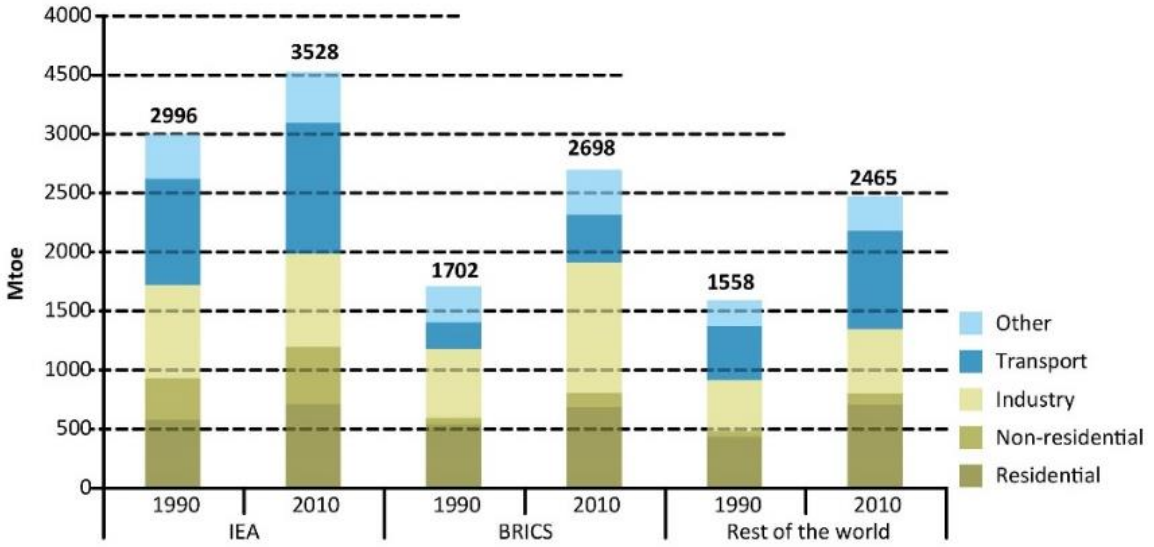


Figure 4. Average annual growth rates of renewable energy capacity and biofuels production, end-2007–2012, based on [8].

Renewable energy plays a key role in reducing greenhouse gas (for example CO_2) emissions and other forms of pollution, diversifying and improving the security of energy supply of humanity and maintaining our world-leading, clean-energy technology industry. That is why the European Union has agreed on legally binding national targets for increasing the share of renewable energy, so as to achieve a 20% share for the entire Union by 2020.

From the viewpoint of the security of supply Hungary is highly dependent on energy source imports, and fulfils 80 % of its domestic crude oil demand, and over 83 % of its natural gas consumption from imports, primarily from former Commonwealth of Independent States (CIS) countries (due to the limited hydrocarbon reserves of the country, the share of imports may increase further). Through the use of renewable energy sources, the dependency on imports can be reduced, as the use of renewable energy is planned to be realised from domestic sources [9].

In the last few years there has been a spectacular growth in using private renewable energy, which has been envisaged by the Hungarian Ministry of National Development. Nowadays, in Hungary, these power stations, which are nominal built in power is less than 50 kW, does not need regulatory or Distribution System Operator (DSO) permission – this is one of the main reasons of growth in renewable energy usage [10] (Fig. 5.).

Energy saving: The most efficient and successful implementation methods to increase the security of supply in the near future are reducing of the primary energy consumption and increasing the energy efficiency [11]. The common aim is increasing the inland primer energy use in Hungary (1085 PJ in 2010) by only 6 % till 2030. But it will not be more than

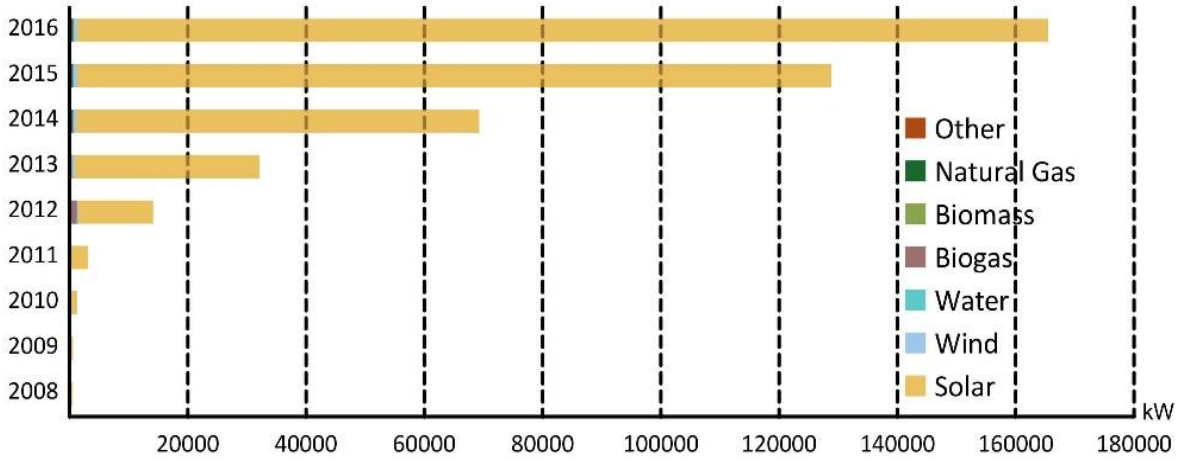


Figure 5. Built in performance of small-scale household power stations according to energy sources, based on [10].

1150 PJ that was the average value in years before the economic crisis. It can be created with the reducing of CO_2 emissions and fossil-energy use [9].

CONCLUSIONS

Environmental sustainability and climate protection: the use of renewable energy sources contributes to the reduction of CO_2 emissions. While selecting specific applications, environmental and nature conservation considerations have special priority. An important mean of ensuring is that environmental and nature conservation aspects are taken into account to include them as criteria for having regarded in particular to the establishment of aid schemes [12].

The most important strategic objective of Hungarian renewable energy policy is to optimise the joint implementation of the security of supply, competitiveness and sustainability as primary national economic goals, while also taking into account long-term considerations.

There can be various forms of interaction between the aforementioned three goals – in many cases their implementation may conflict with one another, but they may also strengthen each other [13].

If the energy consumption reaches the amount of 1150 PJ, the energy intensity will drop rapidly because of increasing of gross national product is associated with an almost stagnant energy consumption. As a result, import dependency of inland fossil-fuels and fluctuation of the energy prices can decrease.

A significant part of energy efficiency increasing is the building energy efficiency program. Nowadays the 40 % of total energy consumption in Hungary is the energy need of the building stock, and two-thirds of it is for heating and cooling. 70 % of the building stock (about 4,3 million) does not fulfil the technical Energy Performance of Buildings Directive (EPBD) requirements. In case of the public buildings this rate is almost the same.

This is the reason of the buildings renovation – most of all in case of public buildings – has priority (because they consume a significant amount of energy). The aim of energy strategy is to decrease about 30 % – 40 % at heating energy demand till 2030 in accordance with guidelines of the EU building energy program. On the other hand, the development of the solar power generation and distribution plays key role in improving energy efficiency, and in reducing energy demand of the industrial and transport sector, too.

REFERENCES

[1] JRC: *National Renewable Energy Action Plans (NREAPs).*
https://iet.jrc.ec.europa.eu/remea/national-renewable-energy-action-plans-nreaps, accessed 13th May 2018,

[2] Minister of Economy: *National Renewable Energy Action Plan*.
Minister of Economy, Warsaw, 2010,
https://ec.europa.eu/energy/en/topics/renewable-energy/national-action-plans, accessed 13th May 2018,

[3] International Energy Agency: *World Energy Outlook 2015*.
International Energy Agency, Paris, 2015,
https://www.iea.org/publications/freepublications/publication/WEO2015.pdf, accessed 13th May 2018,

[4] REN21: *Renewable energy policy network for the 21st century*.
Renewables 2017, Global Status Report, 2017,
http://www.ren21.net/wp-content/uploads/2017/06/17-8399_GSR_2017_Full_Report_0621_Opt.pdf, accessed 13th May 2018,

[5] REN21: *Renewable energy policy network for the 21st century*.
Renewables 2016, Global Status Report, 2016,
http://www.ren21.net/wp-content/uploads/2016/05/GSR_2016_Full_Report_lowres.pdf, accessed 17th May 2018,

[6] International Energy Agency: *World energy outlook 2012.*
International Energy Agency, Paris, 2012,
https://www.iea.org/publications/freepublications/publication/English.pdf, accessed 17th May 2018,

[7] Baranyai, B. and Kistelegdi, I.: *Energy management monitoring and control of public buildings.*
Pollack Periodica **9**(2), 77-88, 2014,
http://dx.doi.org/10.1556/Pollack.9.2014.2.8,

[8] International Energy Agency: *Modernising Building Energy Codes.*
International Energy Agency, Paris, 2013,
https://www.iea.org/publications/freepublications/publication/PolicyPathwaysModernisingBuildingEnergyCodes.pdf, accessed 17th May 2018,

[9] Ministry of National Development: *Renewable Energy 2010–2020.*
Deputy Secretariat of State for Green Economy Development and Climate Policy for the Ministry of National Development, Budapest 2011,
http://2010-2014.kormany.hu/download/6/b9/30000/renewable%20energy_republic%20of%20hungary%20national%20renewable%20energy%20action%20plan%202010_2020.pdf, accessed 17th May 2018,

[10] Hungarian Energy and Public Utility Regulatory Authority: *Summary about the data of small power plants not subject to authorization, including household size (2008-2016).*
Budapest, 2017,
http://www.mekh.hu/download/7/15/40000/nem_engedelykoteles_es_hmke_%20beszamolo_2016.pdf, accessed 18th May 2018,

[11] Olaszi, B.D. and Ladanyi, J.: *PV system auto-sizing with battery energy storage based on GPS coordinates*.
Pollack Periodica **12**(2), 29-41, 2017,
http://dx.doi.org/10.1556/606.2017.12.2.3,

[12] Hungarian Ministry of National Development: *Hungary's National Energy Efficiency Action Plan until 2020*.
Budapest, 2015,
https://ec.europa.eu/energy/sites/ener/files/documents/hungaryActionPlan2014_en.pdf, accessed 17th May 2018,

[13] Hungarian Investment and Trade Agency: *Energy Sector and Renewable Energy*.
Budapest, 2014.

Interdisciplinary Description of Complex Systems 17(1-A), 58-66, 2019

SAFETY ASSESSMENT AND BLAST PROTECTION OF SELECTED SOFT TARGET

Lucia Figuli*, Zuzana Kubíková and Matúš Ivančo

University of Zlin, Faculty of Security Engineering
Zlin, Slovakia

DOI: 10.7906/indecs.17.1.8
Regular article

Received: 31 October 2018.
Accepted: 31 December 2018.

ABSTRACT

The article deals with safety assessment of the building which can be considered as soft target. The building can be a place of the future bomb attack. The article specifies assessment of such blast loaded structure based on the maximal value of the pressure on the window, as crucial part of structure, and the level of possible injury of people. At the end blast protection of selected object is design. The aim of the article is to show the possible threat of persons in the building of Žilina University canteen where a social event takes place.

KEYWORDS

blast wave, bomb attack, debris, windows resistance, safety

CLASSIFICATION

JEL: Q55

*Corresponding author, η: lucia.figuli@fbi.uniza.sk; +421 41 513 6155;
Univerzitná 8215/1, 010 26 Žilina, Slovakia

INTRODUCTION

Over the last few years, the number of terrorist attacks in Europe has increased considerably, causing considerable tension and nervousness. Not only in Europe, but around the world, terrorist attacks and other violent crimes are increasingly concentrated in the vicinity of targets that are easy to access, characterized by a high concentration of people and a relatively low level of protection – soft targets and critical infrastructure that make us more concerned with protecting and defending these goals. With theoretical aspects of critical infrastructure protection deal Hofreiter and Zvaková [1].

Due to the activities of Slovakia, it is not excluded that some terrorist cell in Europe decides to attack our state as revenge for the activities of Slovakia in the global fight against terrorism. However, due to the overall Slovak atmosphere and the position of Slovakia, it is more likely to increase radicalism either in the form of right-wing radicals, religious conservatism or fundamentalism, but also in the activities of individuals with the aim of combating the lack of society (such as the legalization of light drugs, registered partnerships of same-sex partners, against inappropriate citizens or immigrants). Recently, such attacks by so called Lone Wolves are unfortunately more frequent, and they are no longer only abroad, but they are already in our territory. On December 28, 2011, at street of Protifašistických bojovníkov in Kosice in the McDonald's fast-food there was an explosion of a trap explosive system that only by chance accidentally did not injure the customers of operation. The attacker's personal goal was to alert on the animals killing [2].

The target of these attacks could become the academic ground as a space for meeting political streams, progressive views, and significant liberalism. Discussions on the prohibition of abortion or, on the contrary, on the legalization of light drugs can cause individuals to intervene and demonstrate their disagreement. Therefore, it is not excluded that the academic ground will become the target of a Lone Wolves' attack in the future. The act of such a "Lone Wolf" can also be a common revenge for unsuccessful college studies.

SOFT TARGETS

With soft targets, many problems are now linked, from the inability to create a single internationally valid definition, to the creation and application of appropriate security system. An increased number of terrorist attacks and other violent crimes is putting pressure on an urgent solution to this issue. Attacks on soft targets have recently become the most used way of influencing government powers and intimidating people.

In order to work on creating an appropriate security system that can be applied to protect selected objects, soft targets need to be properly defined. Despite the absence of a definition, the concept of soft targets generally refers to people, people assemblies, and objects in which a large number of people are concentrated, these objects are not at all or insufficiently protected against terrorist attacks and other violent crimes.

Based on the above , we can consider as a soft target:

- schools, school facilities (gymnasiums, dining rooms, dormitories etc.),
- Sports facilities
- shop centre,
- theatres and cinemas, concert halls,
- bureau,
- cafes, restaurants, bars,
- churches and church monuments,
- markets and fairs,

- polyclinics and hospitals,
- hotels,
- square,
- museums and galleries,
- train and bus stations, airports, ports, train sets, airplanes,
- various gatherings of people.

These objects are also specific because we talk about them as soft targets only in relation to serious incidents (violent crime – such as mass shooting) or terrorist attacks against which they are poorly protected. This means that in the case of other types of crime, such as property crimes, they are / can be adequately protected (they have a quality camera system, alarm security and emergency systems, physical protection, ...).

The identification of risk soft targets that could become the target of the attack is very important, but at the same time it varies depending on the particular local environment under consideration. For the purpose of this article, we studied soft targets in the local environment of Žilina city. Using the CARVER method to identify important and very important things (objects), we identified as a risky soft target in the city of Žilina the building of Canteen of the University of Žilina.

OBJECT DESCRIPTION

The building of the University Canteen of University of Žilina is the scene of various cultural and social events. Recent social event, connected with celebrations of the 65th anniversary of the founding of the University of Žilina, where hosted over 600 former and current members of the academic community. The canteen of University of Žilina is shown in Fig. 1.

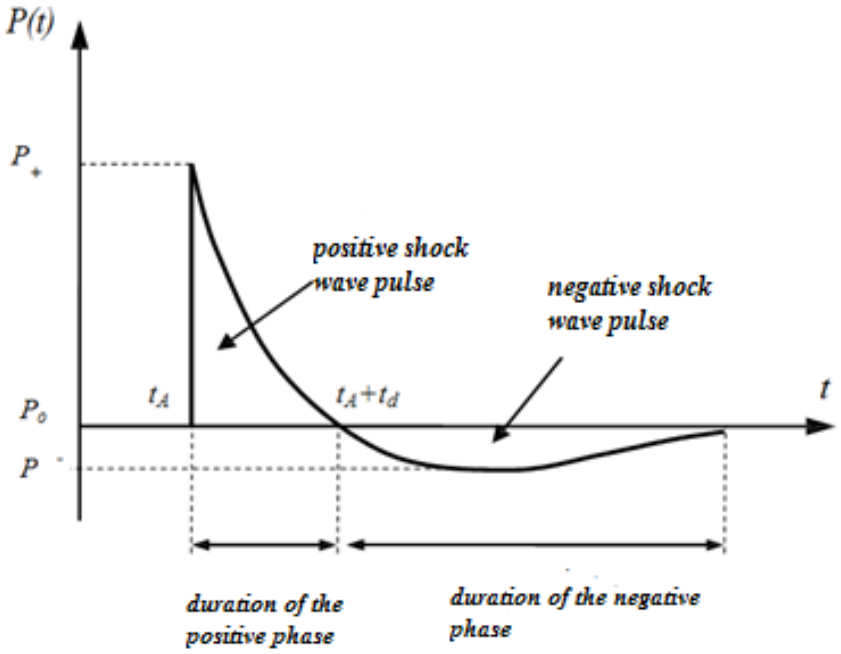
The building is located on the street Vysokoškolákov 26 in Žilina. It is situated in a forested area in a mild hill. There are three access roads to the building, one designed for cars and two for pedestrian access. Due to the large number of students and tearchers and other personels eating daily in this facility, the potential risk of the attack is a great.

Structure of the building consists of fenestration (glazing) and bearing pillars. The glazing is composed of a series of 32 glass panes with two glasses in frames made of plastic profiles reinforced with galvanized steel. The height of the glass wall is 354 cm and the width is 704 cm. In the case of a bomb attack the most vulnerable part of the building to the violation and the subsequent threat to the population are glazed walls. For these reasons we will focuse on the fenestration.

Figure 1. Fenestration of the surveyed structure.

BLAST WAVE PROPAGATION

In the case of initiation of a explosion system, a very strong exothermic reaction occurs. During the reaction, the solid and liquid component of the explosive gas is transferred to the high pressure gas. Explosive products are expanded into the environment under high pressure and strive to find balance with the surrounding environment, resulting in a shock wave. This is characterized by a change in pressure, density and temperature on its frontage. The shockwave process is characterized by a steep increase in pressure at the beginning of its course. Once the maximum value has been reached, the phase goes down, which continues until the negative phase produces a vacuum for a very short period of time, resulting in the drawing of the vapor and air from the environment towards the epicenter of the explosion. Upon leveling, a positive shock wave occurs, but no more than the first recorded pulse. The entire process is generated at very short time intervals, in the order of hundredths of a second [3].



P_0 – initial (zero) value of pressure
P_+ – maximal pressure
P_- – minimal pressure
t_A – arrival time of blast wave
t_d – duration of blast wave

Figure 2. Propagation and phase of pressure wave [3].

During the blast wave, we recognize the two phases – positive and negative. The size of the negative phase pressure is much smaller than in the previous positive part. In analyzes of determination of the response of a construction structure when initiating a explosive system, it is contemplated to idealize the course of the pressure wave to the triangular waveform, i. e. linear function. In further analyzes, such function will be considered.

WINDOWPANE FAILURE

Two cases may occur when the window is damaged. Either the glass breaks or the entire window pane is thrown out.

The breaking of the window panes, when the pressure wave is applied, occurs if one achieves either the bending strength of the glass or the critical angle of the window pane. The removal of the entire window structure from brick or other wall construction material determines how is secured the shear load bearing capacity of the window-to-wall connection. The draw-off of the entire window wings determines on the direction of the load on the window wing and the shear strength of the window frame tructure and further the tensile or shear or bending strength of the hinges according to the arrangement of the entire window structure [4].

The possible deflection of the glass is also the deformation of the window leaf by bending. If the bending capacity of the frame is exceeded, the window frame may break. In case of large deformations, therefore, the bending capacity of the glass is exceeded, resulting in horizontal cracks at the point of greatest stress and thus in the reduction of the load-bearing capacity of the whole window pane [4].

How much pressure is created and the construction is affected by explosion it depeans on many parameters. The basic parameter is the type of explosive substance, the weight of the explosive and the distance from the building. It is decisive how the pressure wave propagates, whether it is perpendicular or oblique, or is reflected or obstructed by an obstacle.

In the bomb attacks mentioned, homemade explosives are used. The worldwide trend is that ammonium nitrate and fuel oil (ANFO) is the most commonly used. Ammonium nitrate is industrially produced in huge quantities and under certain circumstances is itself capable of explosion. With a small amount of fuel added, its sensitivity and explosive properties increase sharply. For our research, we have selected the factory-produced called DAP-2, which has the same properties, as a substitute for the homemade ANFO explosives.

The explosive is a mixture of ammonium nitrate, kerosene and dye. Its detonation velocity is 2 600-2 700 m/s and the explosion heat is 3 830 kJ/kg. At a density 0,65 g/cm^3 the PCJ detonation pressure is 2,95 GPa. With resistance of the object from the effect of explosion of homemade ANFO explosive deal Zvaková and Kavický [10].

Therefore, to determine the maximum value of the overpressure of such a window pane can be made in two ways. When exact mechanical properties of the glass are known, calculating its ultimate strength, i.e. flexural strength, or as mentioned, the angle of the window pane break is possible. In our case, we do not know the precise mechanical properties of the glass used and therefore we will proceed according to the research of Makovicka [4].

Window failure can be estimated from nomograms (Figure 3) based on experimental and theoretical analysis of window glasses under triangular overpressure of blast wave. The maximum overpressure size depends on the size of the glass surface, the glass age (differentiates new and old glass, 10 years), the thickness of the glass and the duration of the overpressure. In our case for 85 × 85 cm^2 = 0,7225 m^2 glass panel, we expect 10-year glass, 3 mm thick.

Using the above mentioned DAP 2 explosive, considering the distance of the pane from the center of the explosion 1 m and the weight of the charge of 0,5 kg, the length of the overpressure is determined by 1,5 ms. From the graph (Figure 3), based on the above values, we determine the size of the wave pressure, which is approximately 10,0 kPa. An explosion of 10,0 kPa will cause damage of the glass. With procedure of the window systems reaction to a shockwave load deals Zvaková in [9].

Ratio of dimensions of window $a/b = 1$.

By the aforementioned procedure, we obtained the maximum pressure that the analyzed pane will carry. In order to suggest possible protection of the object and people, it is necessary to find out what type of explosive, how much weight and distance will cause such explosion. Several approaches from different authors exist to determine strength. We will describe the procedure according to Mills [3]:

$$P = \frac{1{,}772}{z^3} + \frac{114}{z^2} + \frac{108}{z} - 0{,}019. \tag{1}$$

This is the law of the third root, which introduces the reduced distance z

$$z = R \cdot W_R^{-1/3}, \tag{2}$$

where R is the distance from the center of the explosion and W_R is the reduced weight of the charge.

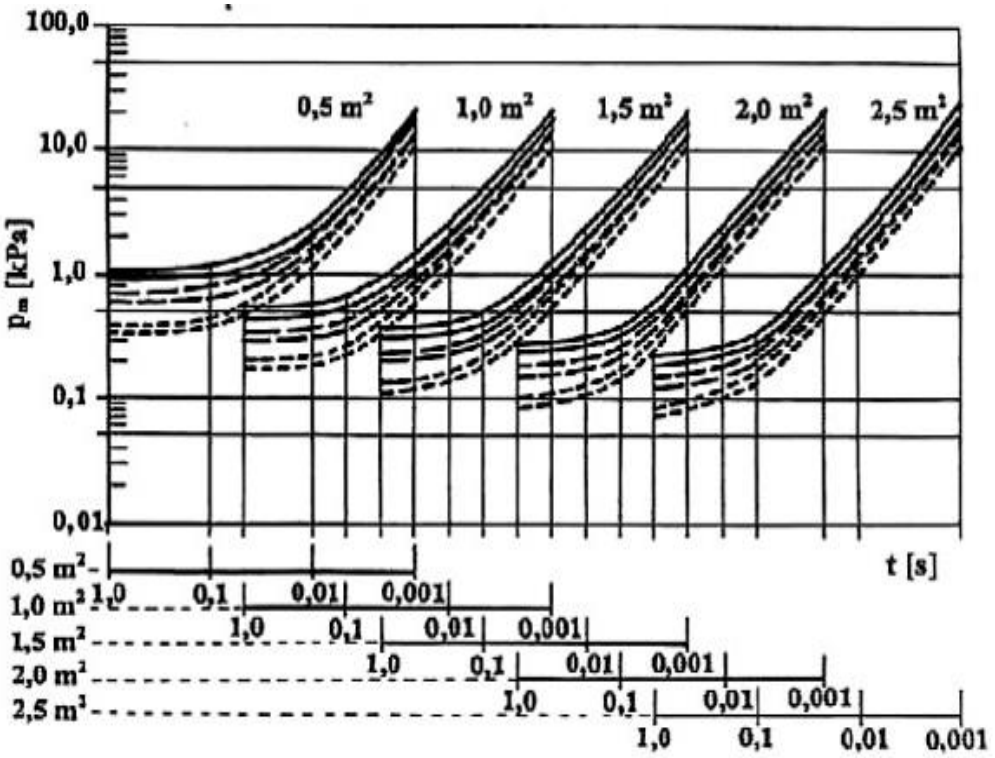


Figure 3. Strength of a window glass [3].

Hence, if the maximum pressure is 10 kPa, from formulas (1) and (2) we obtain that a pressure of 10 kPa on the pane is created with 0,5 kg of DAP 2 explosive at the distance of 10 m. Thus stand-off distance is very critical. It is clear from Table 1 that the closer the source of the explosion is, the greater pressure on the structure is induced. At a very close distance, the pressure increases markedly. The second part of the table shows the pressure-to--weight ratio. From these values, it is possible to assure a devastating effect of the explosive, even with a small amount of the explosive if it is close to the construction.

Table 1. Influence of change of pressure of the explosive system on the distance and weight of the charge.

distance, m	10	8	6	4	2	1	0,1
pressure, kPa	9,77	13,00	19,45	37,60	159,42	958,58	815 532,00

weight, kg	0,5	1,0	1,5	2,0	4,0	6,0	8,0	10,0
pressure, kPa	9,77	13,14	15078,00	1801,00	25,77	32,27	38,14	43,67

As well as window panes, window frames have been experimentally verified. Table 2 was compiled to estimate the strength of the window frames [4].

Table 2. Damage to buildings at various pressures [4].

Pressure, kPa	**Effect**
< 0,5	No damage
0,5 – 1	Small damage to window fills (only part, glass cracks without debris, etc.)
1 – 2	Greater damage to window fills, partial wiping of glass wreckage)
2 – 5	Partial damage to door and window frames, façade and interior wood partitions
5 – 20	Window destruction, damage to light structures and common brick structures
10 – 30	Partial disruption of the buildings of mostly family houses
20 – 30	Significant disruption of urban multi-story buildings

INJURIES OF PERSONS

In the previous calculations, the pressure required to destroy the windows was set to 10 kPa. From Table 3, it follows that the standing person will be buried in the level of 15 kPa. As we suppose, people staying in the dining room behind the window panes, will be damaged by the secondary, by flying out fragments of the windows. Because the structure is not sufficiently resistant to destruction and structure breakage, fragments penetrate into space in the direction of shockwaves and threat the persons. Especially dangerous are small overpressures in the range of 5 kPa to 20 kPa, in which it is highly probable that people will be wounded by wreckage (at a great distance of tens to hundreds of meters) of broken glass windows and doors, at this pressure the slags are not thrown to the ground, [4]. Extreme fragments of different sizes are created by the shock wave effect, resulting in interruptions in the integrity of the window panel, which are capable of acting on a relatively large area. Flying glass fragments most often cause traumatic injuries or penetrate human bodies that are unable to withstand this kind of action. Larger objects coming from damaged building materials cause a devastating injury caused by a combination of weight and speed of the body [5].

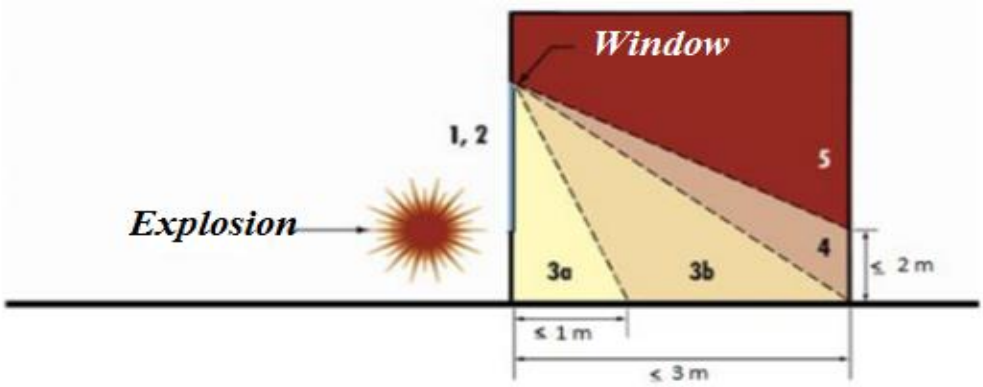


Figure 4. Areas of varying degrees of injury caused by fragments of broken glass [5].

In order to determine the possibility of damage caused by glass fragments, a scale of injuries can be used from a material viewpoint and a method of solving the window filler. The scale has several points. The difference between stages 3a-3b represents the boundary level of injury, where the severity of the point 3b derives the assumption of injury to persons exposed to the cracks created by the window fillers. Another level can be determined at the point between points 4 and 5, where people at the place indicated by point 5 have very serious or even fatal injuries [5].

Table 3. Injury of persons at various pressures.

Vulnerability Group	Overpressure, *P*, kPa	Description of the injury	
0	< 10	Damage from the direct action of the pressure wave is unlikely	
1	10 – 30	Easy injuries to people	At a pressure of approx. 15 kPa, the standing person is buried
			At a pressure of about 34 kPa, the earbuds will crack
2	30 – 150	Severe injuries to persons	
3	150 – 200	Fatal injuries	

PROTECTION DESIGN

A potential bomb attacks is very difficult to predict, but due to the unfavorable current situation in the world and the increasing number of anonymous threats, appropriate protection

features have to be applied. One solution could be the installation of protection against waves caused by an explosive system. The bomb attack will cause considerable damage to the building, which means disturbing the bearing system of the entire building. One solution is to use additional material (so called terofit technique) to increase building resistance. By using recyclable materials they have dealt with research Figuli, L. et al. in [6]. The solution will be the PAXCON PX3350 protective spray application for bearing walls (Figure 5). This type of spraying is used to dampen the action of explosive ammunition, is particularly suitable for enhancing building resistance – significantly reduces secondary damage. The PX 3350 is spray-applied and applied to the walls of a building that is exposed to the risk of a bomb exploding. Spray walls resist explosions due to their ability to bend, ultimately resisting explosions much larger than normal uncoated walls [7].

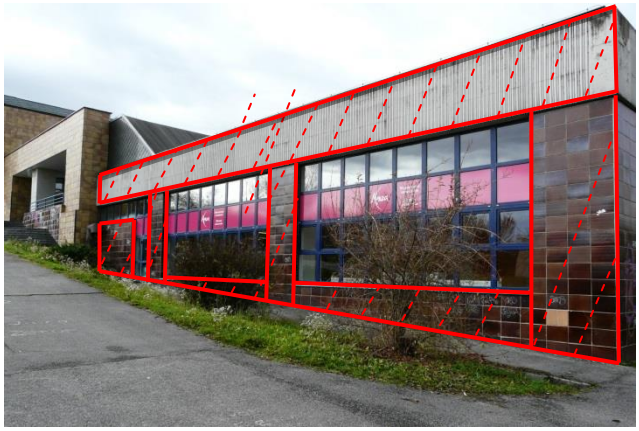


Figure 4. Application of PAXCON PX3350 [9].

Figure 5. Installing security films [9].

Subsequently, because of the large glazed part of the building, it is necessary to install safety glasses for windows, which prevent the glass from breaking into the interior of the building. Security window films are polyester or PET films that are applied on glass surfaces, in order to hold together possible shatters after glass cracking. The main advantages of security films is that they can be applied on glass after manufacture or installation (Figure 6), i.e. in the form of pure retrofitting product. These films are available in various thicknesses, generally in the order of 100 μm, up to 525 μm [7]. For the better protection of present people, special bomb blast net curtains and catchers are intended to protect people inside buildings from exterior explosions. The nets cover windows inside buildings and are aimed to catch and retain flying shards of glass, preventing the whole glass panels from being dislodged by blast wave.

CONCLUSION

When we determine the maximum pressure load that the windows transfer to the building of Canteen of University of Žilina, we have come to various partial conclusions. An overpressure value caused by 10 kPa explosion to which the window pane is low. Such a pressure in itself will not cause very serious personal injury. Persons will, despite this claim, be seriously threatened and injured due to the secondary effects of fragments of broken glass. A pressure of 10 kPa can already develop a 0,5 kg DAP 2 load at a distance of 10m from the building. In order to protect the population and the building, effective action should be taken to prevent catastrophic consequences, to increase the strength of window panes, to prevent access to the immediate vicinity of the windows.

ACKNOWLEDGMENT

This work was supported by the research projects VEGA Nr. 1/0240/15 "Process model of critical infrastructure safety and protection in the transport sector".

REFERENCES

[1] Hofreiter, L. and Zvaková, Z.: *Theoretical aspects of critical infrastructure protection.* In: *Durability of Critical Infrastructure, Monitoring and Testing*. Lecture Notes in Mechanical Engineering. Springer Nature, Singapore, 2016, http://dx.doi.org/10.1007/978-981-10-3247-9_16,

[2] Bejda, R.: *Kosice Terrorists sentenced to 25 years in prison.* http://kosice.korzar.sme.sk/c/6840390/kosickeho-teroristu-odsudili-na-25-rokov-vazenia.html#ixzz2pVvOFrVc, accessed 20th March 2018,

[3] Jangl, Š. and Kavický, V.: *Ochrana pred účinkami výbuchov výbušnín a nástražných výbušných systémov*. Žilina, 2012,

[4] Makovička, D. and Makovička, D: *Odezva konstrukce budovy a ohrožení jejich obyvatel výbuchem plynu.* Stavební obzor **7**, 197-202, 2006,

[5] Vysocký, M.: *Odolnosť materiálov proti nástražným výbušným systémom*. M.Sc. Thesis. University of Zlin, Zlin, 2012,

[6] Figuli, L. et al.: *Application of recyclable materials for an increase in building safety against the explosion of an improvised explosive device*. Advanced Materials Research **1001**, 447-452, 2014,

[7] –: *PAXCON – LINE-X*. Westlake Publications Ltd., 2010, http://www.militarysystems-tech.com/suppliers/military-spray-applied-force-protection/paxcon-line-x, accessed 20th March 2018,

[8] Figuli, L. and Bedon, C.: *An Overview on Current Methods and Trends for Enhancing the Blast Resistance and Protection of Existing Windows*. Transport Means **4**, 2017,

[9] Zvaková, Z.: *Test procedure of the window systems reaction to a shockwave load.* In: *Production management and engineering sciences*. Routledge & GSE Research, Leiden, pp.577-581, 2016, http://dx.doi.org/10.9774/GLEAF.9781315673790_100,

[10] Zvaková, Z. and Kavický, V.: *Odolnosť vybraných prvkov ochrany objektu pred účinkom explózie podomácky vyrobenej ANFO trhaviny.* In: Proceedings of the XXV. International Conference *Združení požárního a bezpečnostního inženýrství*. Klecany, 2016.

Interdisciplinary Description of Complex Systems 17(1-A), 67-77, 2019

PROTECTED SPACES IN SMART CITIES AND THE IDENTIFICATION OF NEW RADIO SIGNALS IN THEIR ENVIRONMENT USING A COMPLEX MEASUREMENT METHOD

Gábor Bréda[1,] * and Péter János Varga[2]

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

[2]Óbuda University, Telecommunications Technology Institute
Budapest, Hungary

DOI: 10.7906/indecs.17.1.9
Regular article

Received: 6 November 2018.
Accepted: 31 December 2018.

ABSTRACT

This research focuses on the creation of a security boundary through the establishment of information security, more specifically by creating an environment that allows for information security for people-to-people communication. The relevance of the research is justified by the vulnerability of infocommunication tools and systems, as well as by the spread of increasingly cheaper information-gathering technologies. There was a need to create an environment where personal, communication between man and man could be realized so that its information content remains protected. Analysing the problem, there are a number of security solutions for information-technology devices, but the creation of a near-human analogue environment for information security is a frontier for the subject. In this approach, the direction of the research was determined by the task of developing an environment that excludes the online operation of infocommunication technologies that create an information security gap and how to identify the spatial position of radio-based communication devices in protected spaces that may be a source of information security. In connection with the continuous quality assurance of the protection, it is necessary to identify the radio signals in the environment of the protected room, which – in the majority of cases – is a built environment with buildings. We offer a new conceptual solution. We studied the operation of the information security breaches during the preliminary research phase by designing a protected space and, by virtue of their principal exclusion, we propose a schematic layout of a protected room, excluding many information security issues. The main purpose of the research is to present an environment that can create a safer person-to-person communication and to provide a novel possible conceptual solution for determining the location of the source of a radio signal.

KEYWORDS

protected room, information protection, protected meeting room, radio direction finding, inertial navigation

CLASSIFICATION

JEL: L63, L94, L96, L98

PACS: 84.40.Ua, 84.40.Xb

*Corresponding author, η: bredagabi@freemail.hu; - ;
H – 1428 Budapest, Pf.:31, Hungary

INTRODUCTION

The development of smart cities has greatly increased the use of wireless technologies. The close-range operation of a large number of radio devices involves the formation of interference and the problem of malfunctioning caused by disturbances. Faults in such malfunctions resulting from this kind of error can be a critical issue for the continued operation of smart cities, as basic infrastructures are built on these devices. Automation systems are everywhere, from positioning and communication functions in traffic through information infrastructure in business, to industrial wireless networks and smart homes [1]. As a result of the subject, a special problem emerges in terms of information security for smart cities. This problem is largely relevant to business and administrative infrastructure as the special physical security interface that could address the problem opposes smarting processes. In order to provide information security, an environment in which oral and visual information is secure is to be established [2]. One way to create security for word of mouth and the visually emerging information is to carry out the interaction between the walls of a protected conference room. The creation of such environment in a Smart environment is a special task because the entire verticality of the telecommunications acquis in the information society must be excluded from such an environment [3, 4]. The physical security of protected meeting rooms includes the need to ensure continuous testing and protection of the direct radio environment. By using a continuous monitoring system in the environment we are able to acquire a picture of the features of the radio ether and the presence of radio communication devices. In such environments, it is necessary to know the frequencies present and their sources and to detect new radio signals. The emergence of a new frequency may pose a security risk because the smart environment is fully covered by the arsenal of wireless telecommunications technologies. The source of the new signal that appears is to be identified in the same way as the source of possible disturbance for smart wireless systems. Protected premises relevant to the subject are in a densely-built environment following urbanization trends where the implementation of radio localization is difficult because of the delimiting walls of buildings and reflections. Researching the subject, the detection of interference of devices using standard wireless communication technology is a well-proven measurement system, but localizing disruptions is a difficult task. With the emergence of the problem, paralleling the complex security of the protected premises, the localization of a radio source may be a problem. This article first aims to provide an overview of the principle of the physical design of a protected conference room we deem appropriate and the principle of the protection of the radio protection, and then, later on, will continue to provide a solution to the problem of the exploration of the radiation source outlined above. The solution comes from the combined use of multiple technologies, which include conventional radio field measurements, inertial navigation, cloud-based data storage and data processing technology, and elements of computer visualization.

Data, that may either be open or undisclosed, is generated 24 hours a day in the information society of our time, as well as in smart cities. Data is usually stored on a data carrier or in an information-technology (IT) system to achieve the appropriate quality and capacity. You have to process data to turn it into information. The data processing and the storage of results are nowadays almost exclusively carried out on computing devices, which significantly increases the relevance of the creation of protection designs for the security of non-public data [5-9]. Data protection is dealt with by the legislator at a legislative level, and the protection of IT tools and networks, as the basic information sharing environment of the information society, is dealt with by development and research teams, as well as international and national organizations [10-16].

METHODOLOGY

In the initial phase of the research, general research methods were used. The review of the problem to be resolved, the examination the physical characteristics of human communication, and the examination of the emerging effects. Thereafter, a search for a conceptual solution to exclude problems that arise, and finally, a proposal was made for a conceptual design. During the research, the question of localizing radio signal sources in environments surrounded by buildings arose. Looking at the subject, it's difficulty became prominent. Analysing the problems that arise during the research, a novel conceptual solution can be proposed for the problem.

The expected outcomes at the end of the study:

- proposal for the design of a protected room,
- investigation of the possibilities of the localization of radio signal sources,
- proposal for the localization of radio signals in the vicinity of a protected room.

CONCEPTUAL DEFINITIONS

"Smart City: A smart or a 'more livable' city is a settlement that uses the technology options available (primarily information and communication technology) in an innovative way that promotes a better, more diversified and more sustainable urban environment. A city may be called 'smart' if sustainable economic development and a further increase of living standards is stimulated and driven by the investment in human capital, traditional (e.g. transport) and modern information and communication infrastructure – while treating natural resources wisely" [17].

According to literature [18]: "Information protection (or information security as defined by the NIST): The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

1. integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
2. confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
3. availability, which means ensuring timely and reliable access to and use of information."

Our conceptual definition of a protected room is as follows. From the point of view of the subject, we define a demarcated area as a protected area where sensitive, valuable data and information (at the right place, classified data, and information) are displayed in an acoustic and visual form. The intended objective is that the data and information that are produced in a protected room should be impossible for unauthorized parties to acquire. The aim is to create and maintain a uniform protection strength.

"Radio direction finding (DF) system: It is an antenna array and a receiver arranged in a combination to determine the azimuth angle of a distant emitter. All DF systems derive the emitter location by initially determining the angle-of-arrival (AOA). Classically, radio direction finding techniques have been based on multiple-antenna systems that employ multiple receivers" [19].

Radio monitoring: an inspection of the radio frequency environment that constantly monitors the characteristics of a radio spectrum in question. It is able to detect radio signals that appear in the examined range and it can indicate if there is a deviation from the reference value in the case of a signal.

"Inertial navigation is a self-contained navigation technique in which measurements provided by accelerometers and gyroscopes are used to track the position and orientation of an object relative to a known starting point, orientation and velocity" [20].

THE EMERGING BREACH IN INFORMATION SECURITY

To ensure that non-public information is displayed (be qualified or sensitive) more criteria must be met. The confidentiality, integrity, credibility, and availability of data, as well as the necessity and proportionality of the protection, and the principle requirement of knowledge [5, 8, 9] must not be violated [4, 21]. In order for data to be interpretable by a human being, one has to elaborate it and get to know it during a process [15]. The information should continue to comply with the data criteria. The processing of protected information usually takes place in a delimited system, as well as in an environment protected by engineering and the previously mentioned laws and organizations. Cognition and sharing in a human-human context require new physical and protective measures to achieve a level of defense consistency. Human cognizance is carried out with the help of sensory organs, especially hearing and vision. The display of information in a form that is directly understandable to man, and is happening in the processor, storage and transmission chains that are considered well protected, encompasses a new medium – the protection of which that cannot be ignored. This medium is the space in which the information is displayed acoustically and visually. Cognition requires interfaces. The physical phenomena appearing in voice-based transmission are either the vibrations of the voice generated by human communication or the sound of a speaker from an IT media player. During visual transmission, the physical phenomena are either the paper with the written information or the information content of the various monitors and projectors. There are several physical phenomena in the chain that need to be investigated from an information security point of view, and in the emergence of a theoretical information security breach resulting from their occurrence, security steps may be needed to be taken to block a possible channel [22]. If stored and transmitted information are provided with a high level of protection in IT and storage systems, then beside the protection of legal, theoretical and IT elements, the physical design of the environment compliant to information security also cannot be neglected, as data and information is displayed there in their purest, most human-close form. With regards to its notion, we call a protected room a demarcated area where the exchange of data and information on data carrier devices, and human-to-human communication can be realized in accordance with the criteria for classified information. During cognition and communication, primary and secondary physical phenomena are created that carry the information itself, thereby opening up the possibility of information leakage. A primary phenomenon is the sound, that makes uses the air pressure waves as a transmission channel to make the eardrum of nearby communicators and the surface of nearby objects vibrate. In the case of visual communication, photons of light are reflected by the written media and are directly emitted by the monitor or projector and travel through the air into the eyes of the participants. Secondary phenomena are magnetic fluxes that correlate with the appearance of information resulting from the operation of equipment used in communication, additional vibrations in the sound generated by the sound, and scattered beams during the reflection of light. In addition, further information security problems may be posed by telecommunication devices at the site of communication, the networks of which now offer almost complete geographical coverage [23]. Based on the data protection criteria and considering the possibilities of technology, it can be stated that in the case of human-to-human communication, and cognition of information with the help of a technology tool, the primary and secondary data generated at the site of the interaction can be intercepted in the absence of adequate protection and thereby the fulfillment of the data protection criteria could be at harm. Sensitive data and information must be processed and distributed to the right holders within the walls of a room, a protected area in which they are secure [24, 25]. The physical phenomena resulting from the various forms of communication and the contributing additional information must be in the plane of the bounding walls of the protected space [26-31].

BASIC DIRECTIVES FOR ESTABLISHING PROTECTED POINTS

The establishment of the security organization of a protected room, or protected meeting room in our case, cannot be conceived without the use of defense resources. Resources, based on their type, can be live solutions and technical protection tools [32-34]. In this research, we focus on the development of physical and technical protection solutions. When establishing a protected room, placement is the first step. The location of such a room should, as an autonomous space, be positioned as an interior space of a building group, with a complete horizontal and vertical interconnection. The physical security of the protected room can be further enhanced when it is surrounded by a fully controlled space. The design proposal is the realization of a shell model, according to which a new autonomous space is created within the designated space, with the realization of special needs. This new partition wall should be made of a material that remains sufficiently firm, even in the case of long-term human presence. In terms of material, breakdown and restoration should not be possible without traces. The space between existing and formed spaces must be permeable from all directions due to the feasibility of subsequent checks. The inner side of the confining outer space has to be shielded in order to dampen the radio signals originating from within the inner space and to prevent access to the communication channels from the outside [35]. The ventilation of the inner room must be solved from the outside room so that the flow of fresh air indirectly arrives at the inner compartment's airspace to avoid contact with the direct outside space. In the space between the two rooms and in the engineering channels, noise has to be generated to prevent the transmission of sound vibrations from the interior room. The walling of the exterior enclosing room must be checked for the degree of acoustic attenuation of the sound that is coming from the interior room, and in the case of weak dampening, it must be sound attenuated [36-38]. The lighting of the meeting room should also be provided with light sources on the walling of the surrounding room, thus reducing the number of technical installations used in the protected room. Considering the furnishing of the meeting room, simplicity should be sought after. Furniture items should contain as little metal as possible, relying mainly on glass and transparent plexiglass furniture, if possible [39]. When designing the protection, the room complex must be secured with proper locking and access control system. When constructing the electronic property protection, it is recommended to create an autonomous camera surveillance system and electronic property protection that is separate from the central defense system. When discussing the comprehensive design of the complex security of protected premises, the monitoring of the radio environment of the room cannot be neglected [32]. In the vicinity of a protected room, it is necessary to know the characteristics of the radio spectrum and the origin of the frequencies found therein. Despite the shell model, an emerging radio signal may still carry a security risk and identify its origin is a must.

One possible information leakage channel in protected rooms is the security vulnerability that emerges due to radio signals. The solution to the problem is the operation of the radio monitoring system, which performs radio spectrum monitoring and analysis. If a new radio signal is displayed in the protected room or in its vicinity, the monitoring system shall generate an indication for the operator. The source of the sign to be displayed needs to be identified to reduce the security risk. Such a room can be seen in Figure 1.

METHODS FOR DETERMINING THE LOCATION OF A RADIO EMITTER

The continuous testing of the radio environment and the detection of the newly emerging frequencies can be done in several ways, but the framework of this study does not allow for it to be explicated. However, it is a tough task to identify the sources of radio signals around the protected areas of smart cities. The localization of a radio source is provided by the methods of radio direction measurement and positioning and their combinations. Listing the methods,

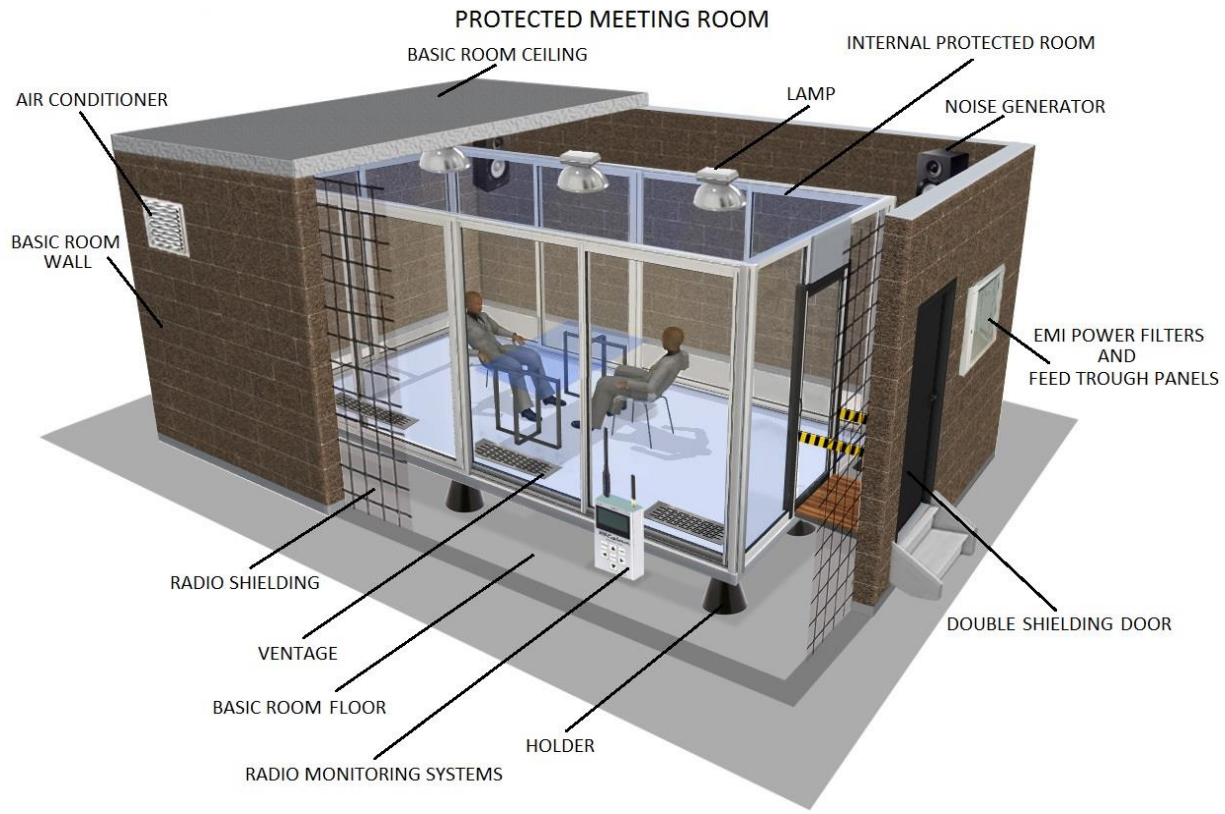


Figure 1. Possible design a protected room based on own idea.

the following options are available. The AOA is measured based on the angle of incidence of the signal. When an antenna is used as a directed spatial filter, the direction of the signal's radiation is measured from a plurality of spatial reference points by direction measurement,

and then the intersection point is calculated or represented to obtain the source position. It can be used with elevated efficacy in densely-built and internal spaces, due to shadowing and reflections [40]. Another solution could be the *Time Difference of Arrival*, the time difference between the arrival of signals, and the *Time of Arrival* measurement method, which is based on measuring the time the signals arrive. The method requires a simultaneous setting of at least three reception points. Because distances are small, high-precision timing and accurate time synchronization between the reception points are a necessity. It is effective when detecting impulse signals.

However, although the methods for outdoor measurements are usually successfully applied, in the event of interference and multiple path signal propagation, they do not give a satisfactory result in every case. In densely built environments and in the interior of buildings, the main problem in the detection of radio signals is their reflection from objects and the scattering of these reflections. To determine the radio source within buildings, a better solution would be to determine signal strength decreases by using the Received Signal Strength (RSS) method. By knowing the damping of the medium, and by measuring the intensity of the incoming signal in different places, and then calculating the distance and attenuation, the source location can be determined by representing the intersection of the circles [19, 41-43]. The increase in damping value in open terrain for an isotropic antenna is proportional to the square of the distance between the transmitter and receiver. Between and within buildings, this value can only be modeled using complex formulas. Depending on the frequency and the built environment, several damping formulas can be written. The literature contains the Okumara-Hata model, which is contained in the expression (1) [44]:

$$PL = 69{,}55+26{,}16\cdot\log(f) - 13{,}82\cdot(h_t - h_r) - c(h_r) + [44{,}9 - 6{,}55\cdot\log(h_t - h_r)]\cdot\log(d), \quad (1)$$

where PL is propagation loss measured in dB, f frequency measured in Hz, d distance between transmitter and receiver measured in m, h_t and h_r transmit and receiving, respectielly, antenna height measured in m, and $c(h_r)$ correction factor, the value of which is as follows:

$$c(h_r) = -\begin{cases} 3{,}2\cdot\log^2(11{,}75\cdot h_r) - 4{,}97; & \text{in a large city,} \\ [1{,}1\cdot\log(f) - 0{,}7]\cdot h_r - [1{,}56\cdot\log(f)] - 1{,}8; & \text{in a small town,} \\ 2\cdot\log^2\dfrac{f}{28} + 5{,}4; & \text{in a suburban area,} \\ 3{,}2\cdot\log^2(f) - 18{,}33\cdot\log(f) + 40{,}94; & \text{in an open area.} \end{cases} \quad (2)$$

Furthermore, the International Telecommunication Union (ITU) prescribed formulas of which ITU-R P.1238-7 02/2012 has been optimized for frequencies above 900 MHz. The term is described in the following expression [45]:

$$L_{total} = 20\cdot\log(f) + N\cdot\log(d) + L_f(n) - 28, \quad (3)$$

where N is a distance power loss coefficient, d separation distance (measured in m) between the base station and portable terminal (with $d > 1$ m), L_f floor penetration loss factor measured in dB and n number of floors between base station and portable terminal ($n \geq 1$).

DETECTION OF RADIO SOURCE IN A DENSELY BUILT ENVIRONMENT WITH THE COMBINED USE OF COMPLEX TECHNOLOGIES

As you can see, attenuation is strongly dependent on the environment. Therefore, it is not easy to determine the location of a radio source, even when using the RSS method, furthermore, navigation within the buildings without a GPS signal is also a challenge. The conceptual layout presented can provide a novel solution to these difficulties. This solution can, in principle, achieve the best results with the simultaneous use of several already existing simple technologies. The implementation consists of a complex measuring unit and a data processing evaluation part. The measuring unit measures its own spatial position and the strength of the set radio signal on the spot. The data processing unit displays the recorded data on a graphical interface to the user. One possible solution to measuring accurate spatial location is inertial navigation. The principle of the operation of inertial navigation systems is based on the application of physical phenomena that occur when accelerated movement of bodies is examined in a standing right-angle coordinate system. Accelerometers are used to measure inertial navigation systems. Nowadays, small size *Inertial Measurement Unit* sensors are available that can be used and are accurate enough to accomplish this task. The sensors perform complex functions in terms of their operation by providing acceleration, rotation and magnetic field data through their output. The coordinates that are absolutely necessary for positioning are calculated from the second integral of the accelerometer timing signals [46-49], see Figure 2.

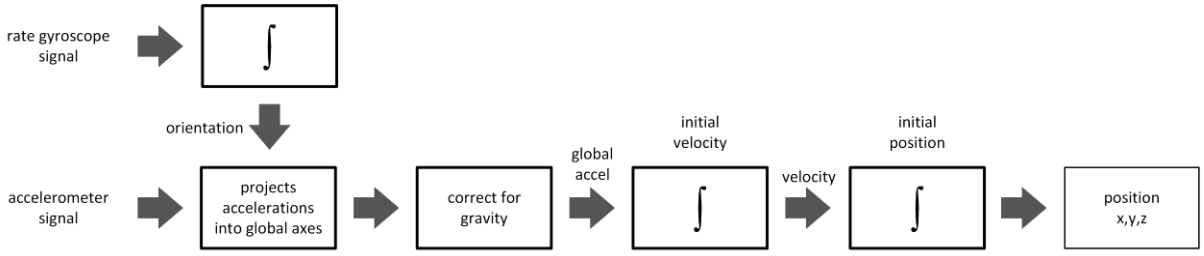


Figure 2. Gyroscope-based positioning [48].

At about the same time, the signal strength and bandwidth signal are determined with a software radio with surround antennas. We assign the values of the strength of the radio signal in the given space to the location data, previously calculated from point to point. The resulting data is transferred to a database. After the data processing, the radio field strength distribution of the area is examined based on a given frequency and is then shown graphically in three dimensions. Visualization can be carried out by matching the combination of various false color and thermal imaging methods with the blueprints and maps of the examined area. The implementation and evaluation of the measurement, in the case of a preconfigured system, does not require special expertise from the people performing the task. The layout principle is shown in Figure 3.

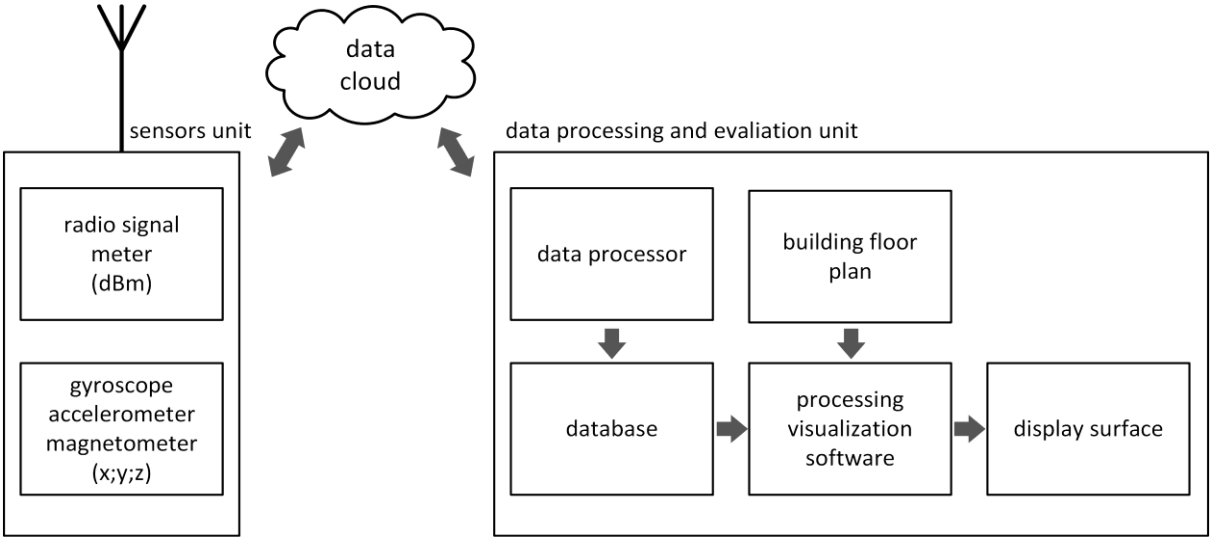


Figure 3. Location-based radio coverage meter layout.

The system consists of two separate units. By analyzing the layout, it becomes obvious that the evaluating display unit does not have to be on the measuring site and the measurementdata can be evaluated offline and online too. The small size of the radio measuring unit, that functions as a probe, allows for it to be easily integrated into a variety of autonomous robots (UAVs, UGVs) so that areas can be mapped quickly to detect the source of the given radio signal. In the following, the practical implementation of the measuring system is to be carried out in connection with the continuation and closure of the research so that we can conclude the feasibility of the theory based on the realistic measured data.

SUMMARY

The data security of human communication that goes on in smart cities carries the heightened risk of data breach, that is cumulatively present due to the opportunities offered by the different technologies. The physical design of protected rooms, which requires the creation of a separate room for the sake of information security is discussed in this article. The space around the protected premises, as a possible data transmission channel, requires the task of continuous control. New radio frequencies near protected areas may be the source of information security hazards, the source of which is to be identified. There are several possible solutions for measuring radio direction and determining transmitter location, however, it is difficult to implement these solutions in built environments, due to the attenuation and multi-path diffusion phenomena. By studying this problem, we would like to offer a novel conceptual solution to the task, which can provide a solution for discovering sources of radio signals in a built environment. The positioning, measuring and evaluation functions used in the measurement fit into the concept of simple implementation that is a typical to smart systems.

ACKNOWLEDGMENT

The research on which the publication is based has been carried out within the framework of the project entitled "The Development of Integrated Intelligent Railway Information and Safety System", application number: GINOP-2.2.1-15-2017-00098.

REFERENCES

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

[2] Lazányi, K.: *The role of safety culture in supporting managerial decisions.*
Taylor Gazdálkodás- és szervezéstudományi folyóirat **1**, 143-150, 2016,

[3] Kuris, Z.: *New directions in complex information protection in relation to the protection of national classified information*.
Hadmérnök **5**(4), 2010,

[4] Lazányi, K.: *The safety culture.*
Taylor Gazdálkodás-és szervezéstudományi folyóirat **1**(2), 398-405, 2015,

[5] –: *2009 CLV. Act on the Protection of Classified Information.*
accessed 1st December 2017,

[6] *90/2010 (III. 26.) Government Decree on the operation of the National Security Supervisory Authority and the handling of classified information.*
accessed 1st December 2017,

[7] *92/2010. (III. 31.) Government Decree on detailed rules for industrial safety inspection and site security certification*.
accessed 1st December 2017,

[8] *161/2010. (V. 6.) Government Decree on detailed rules for the electronic security of classified information and the authorization and regulatory oversight of concealed activities.*
accessed 1st December 2017,

[9] *Act L of 2013 on Electronic Information Security of Public and Municipal Bodies.*
accessed 1st December 2017,

[10] GovCERT-Hungary.
http://www.cert-hungary.hu, accessed 1st December 2017,

[11] Marshall, D.A.; Sushil, J.J. and Podell, H.J.: *Information Security: An Integrated Collection of Essays*.
IEEE Computer Society Press Los Alamitos, 1995,

[12] *ISO/IEC 20000-1:2011 Information technology – Service management.*
https://www.iso.org/standard/51986.html, accessed 1st December 2017,

[13] 2011 CXII. *Act on the Right to Information Self-Determination and Freedom of Information*.
accessed 1st December 2017,

[14] ISO: I*SO/IEC_27000-series, Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
https://www.iso.org/standard/73906.html, accessed 1st December 2017,

[15] Ackoff, R.L.: *From Data to Wisdom.*
Journal of Applied Systems Analysis **16**, 3-9, 1989,

[16] IBM Global Business Services Executive Report: *Smarter cityes for smarter groeth; How cities can optimize their systems for the talent-based economy.*
IBM Global Business service, Executive report, IBM Institute for Business Value, 2010,
http://www.zurich.ibm.com/pdf/isl/infoportal/IBV_SC3_report_GBE03348USEN.pdf, accessed 1st December 2017,

[17] Lados, M.: *Cities for Smarter Growth*.
IBM Institute for Business, 2011,

[18] Lord, N.: *Information Protection vs. Information Assurance: Differentiating Between Two Critical IT Functions*.
Digital Guardian, 2016,
[19] Nisar, A.: *Radio Direction Finding: Theory and Practices.*
https://www.researchgate.net/profile/Nisar_Ahmed10/publication/289779492_Radio_Direction_Finding_Theory_and_Practices/links/569e752508ae21a56424b5a2/Radio-Direction-Finding-Theory-and-Practices.pdf, accessed 1st December 2017,
[20] Woodman, O. J.: *An introduction to inertial navigation*.
https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-696.pdf, accessed 1st December 2017,
[21] Kuris, Z.: *Approaching Complex Information Security Implementation Options*.
Hadmérnök **4**(2), 311-318, 2009,
[22] Tokody, D. and Mezei, I.J.: *Creating smart, sustainable and safe cities*.
2017 IEEE 15th International Symposium on Intelligent Systems and Informatics, 14-16 Sept. 2017. IEEE, Subotica, 2017,
[23] Ványa, L.: *Modernizing electronic warfare assets, systems and management in the face of new challenges, in particular electronic countermeasures.*
[24] Haig, Zs.: *Complex Interpretation of Information Security, Robotage 6.*
http://hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.pdf, accessed 1st December 2017,
[25] Kerti, A.: *Examination of the technical subsystem of the management and information system with special regard to quality assurance and transmission security.*
Miklós Zrínyi University of National Defense, 2010,
[26] Muha, L.: *Protecting critical information infrastructures of the Republic of Hungary.*
Miklós Zrínyi University of National Defense, 2007,
[27] Haig, Zs.: *Information-based threats to the information society.*
Hadtudomány **17**(3), 2007,
[28] Rajnai, Z. and Fregan, B.: *Critical Infrastructure Protection.*
Proceedings of the XXI. International Scientific Conference of Young Engineers, pp.349-352, 2016,
[29] Vadász, P.: *Competitive intelligence as a branch of economic intelligence.*
Hadmérnök **9**(2), 343-357, 2014,
[30] Varga, P.J.: *The critical infrastructure and critical information infrastructure*.
Hadmérnök **3**(2), 149-156, 2008,
[31] Keszthelyi, A.: *Information security, basic technical knowledge.*
Vállalkozásfejlesztés a XXI. században, pp.303-340, 2012,
[32] Berek, L.: *Security systems.*
Nemzeti Közszolgálati Egyetem, Budapest, 2014,
[33] Berek, L.; Berek, T. and Berek, L.: *Person and property security textbook.*
Óbudai Egyetem, Budapest, 2016,
[34] Boros, B. et al.: *Law enforcement, property protection.*
BME, Budapest, 1997,
[35] –: *Information on the tasks of the National Security Supervisory Authority and on the qualification of electromagnetic radiation protection on the Internet*.
http://www.nbf.hu/tempestmer.html, accessed 1st December 2017,
[36] Töltési, I.: *Monitoring protection in business 1*.
Detektor plus folyóirat, pp.32-33, 2006,
[37] Töltési, I.: *Monitoring protection in business 2*.
Detektor plus folyóirat, pp.58-59, 2006,
[38] Töltési, I.: *Monitoring protection in business 3.*
Detektor plus folyóirat, pp.47-49, 2006,
[39] Vaszari, Á.: *Business Intelligence for Multinational Companies and Small and Medium Enterprises.*
Budapest Technical College, Budapest, 2007,
[40] Karl, R.: *Antenna book.*
Műszaki Könyvkiadó, Budapest, 1977,

[41] Németh, Zs.: *Locating on wireless networks*.
BME, Budapest, 2009,

[42] –: GOP 1.1.1-11-2011-0048 *Examination of localization methods, protocols and their applicability.*
http://www.corvex.hu/files/3214/2668/9380/R14AB_Lokalizacios_modszerek_protokollok_es_alkalmazhatosaguk.pdf, accessed 1st December 2017,

[43] Paul, D.: *An Introduction to Radio Direction Finding Methodologies.*
https://wireless.vt.edu/symposiumarchives/2015_slides/document.pdf, accessed 1st December 2017,

[44] Takács, Gy.: *Positioning with mobile phone and mobile network.*
Híradástechnika **63**(8), 20-27, 2008,

[45] International Telecommunication Union: *Recommendation ITU-R P-1238-7: Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 900 MHz to 100 GHz.*
https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.1238-7-201202-S!!PDF-E.pdf, accessed 1st December 2017,

[46] Kornél, Gy.; Varga, P.J. and Illési, Zs.: *WLAN heat mapping in hybrid network.*
In: Novitzká, V.; Korečko, Š. and Szakál, A., eds.: *Proceedings of the 2017 IEEE 14th International Scientific Conference on Informatics*. IEEE, Poprad, pp.94-97, 2017,
http://dx.doi.org/10.1109/INFORMATICS.2017.8327228,

[47] Smalling, K.M. and Eure, K.W.: *A Short Tutorial on Inertial Navigation System and Global Positioning System Integration*.
https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150018921.pdf, accessed 1st December 2017,

[48] Woodman O.J.: *An introduction to inertial navigation.*
Technical Report UCAM-CL-TR-696, University of Cambridge, 2007,
https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-696.pdf, accessed 1st December 2017,

[49] Cveticanin, L.; Mester, Gy. and Biro, I.: *Parameter Influence on the Harmonically Excited Duffing Oscillator.*
Acta Polytechnica Hungarica **11**(5), 145-160, 2014.

Interdisciplinary Description of Complex Systems 17(1-A), 78-84, 2019

SMART SOLUTIONS AND OPPORTUNITIES FOR DISTRICT HEATING: THE CASE OF BUDAPEST

András Horkai[1,] *, Balázs Némethi[2] and Attila Talamon[1]

[1]Szent István University, Ybl Miklós Faculty of Architecture and Civil Engineering
Budapest, Hungary

[2]FŐTÁV Budapest District Heating Works Private Co. Ltd.
Budapest, Hungary

DOI: 10.7906/indecs.17.1.10
Regular article

Received: 31 May 2018.
Accepted: 31 December 2018.

ABSTRACT

The smart city, as a phenomenon, primarily focuses on citizens, city services, decision making mechanisms and information technology solutions, with various criteria such as sustainable development, economic efficiency and broad participation. One of its subsystems is the Smart Environment, which among others, aims for decreasing energy consumption and increasing energy efficiency of the built environment: to make energy processes more sustainable (renewable energies, water management), and circular processes utilizing resources.

District heating is one of the most environmentally friendly and modern method of heat supply (with concentrated emission and efficient power supply of renewable energies), which is present in the heat market of Budapest with a share of about 30 %. District heating supplier of the capital city (FŐTÁV) provides to nearly quarter million dwellings.

Present article focuses on the district heat supply in Budapest, the use of resources and renewable energies and demonstrates the investments of the high-efficiency cogeneration facilities according to the EU directive on the heat producer's side. The article also presents public energy saving tenders in district heating in the capital so far: I LOVE PANEL and OKOS-HÁZAK project.

KEY WORDS

Budapest, district heating, energy saving, smart environment

CLASSIFICATION

JEL: Q41

*Corresponding author, η: horkai.andras.laszlo@ybl.szie.hu; +36 30 490 3878;
Budapest, Thököly út 74., H-1146, Hungary

INTRODUCTION

In Hungary, 60 % of the energy consumption of buildings is provided by residential buildings; 35 % provided by public buildings, service and commercial buildings; industry and agriculture are present in low shares (about 5 %) [1].

In 2016, Hungary contained 649 129 dwellings [2], which have been practically unchanged for many years. District heating units account for 14,68 % of the domestic housing stock, representing a considerable proportion [3].

In Hungary, the goals of the National Building Energy Strategy [1] include: increasing energy efficiency and renewable energy utilization in district heating: investment not only for building renewals, but also for energy efficiency interventions, for example: measurement accounting, modernization of substations, renewable energy applications. These activities result in additional energy savings beyond the effects of building renovations, and the strategy plays a key role in consumer awareness, consulting and information exchange [1].

In this article, the authors introduce and analyse the smart solutions and development opportunities that have been realized and planned for the district heating supply from the producer's side and with the involvement of the household consumers in Budapest.

SMART CITY AND SUBSYSTEMS

The concept of a smart city focuses on services, information technology solutions and decision-making mechanisms along the lines of sustainability, efficiency and broad-based development priorities. This expression is one of the key phenomena of economic innovation and contemporary urban development, the integration of cities and digital technologies [4, 5].

"A smart city is a settlement or a group of settlements, which develops its natural and built environment, digital infrastructure, and the quality and economic efficiency of its locally available services by adopting novel and innovative information-technologies, in a sustainable way, through the increased involvement of its residents" [6].

The Smart City Ranking and the Smart Cities Council index system specify six subsystems in smart cities to measure the development of cities and the impact of smart city projects: smart governance, smart traffic, smart environment, smart economy, smart living conditions, and smart people [6].

From the point of view of district heating supply and building energy, the two most important subsystems are the smart environment and smart people.

Smart environment covers sustainable environmental resource management (renewable energy, water-, and waste-management), measures to improve the air quality, increasing urban resilience and adaptation to climate change, and the energy-efficient development of the built environment [6].

Smart people covers the strengthening of the knowledge economy and a competitive labour force, programs supporting lifelong learning and innovation in education, measures taken to establish a creative and inclusive society such as participatory planning, co-production and co-design processes [6].

In the relationship between these two subsystems, it is important to increase the energy awareness of the consumers (smart people subsystem) to ensure sustainable management of environmental resources and thus to make our environment more energy-efficient (smart environment subsystem).

DISTRICT HEATING SUPPLY IN BUDAPEST

District heating is an environmentally friendly, modern heat supply method that represents approximatelly 30 % of the capital heat market (this 30 % is owned by Budapest District Heating Works Private Co. Ltd. (Hungarian: FŐTÁV). Over the past decade, high-efficiency cogeneration facilities have been built on the producer's side in accordance with EU directives.

FŐTÁV operates nine separate, hydraulically independent (unconnected) district heating zones and four block-heating [7]. The connection of the systems has been partially completed and partly planned. The relative heat loss of heat transfer and distribution systems – partly due to continuous upgrades – is approx. 10-11 %, which is 1-2 percentage points below the European average. Most of the substations supply a building or section, and accordingly their metering and control functions are connected to the provided area. The least effective points of the district heating system are the insufficient heat insulated buildings with high energy consumption and the outdated secondary systems owned by the consumers. Due to their market-retention and market expansion goals, the district heating provider also plays a role in modernizing them [7].

SMART SOLUTIONS FROM THE PRODUCER'S SIDE

NORTH-PEST HEAT COOPERATION AND ENERGETIC USE OF HOUSEHOLDS WASTE

The amount of heat generated by the energy utilization of household waste (0.5 PJ per year) reaches half of the district heating energy demand of Hungarian rural cities (e.g. Nyíregyháza, Székesfehérvár). However, which share now rising to 5% is still rather low, especially with the 3,2-3,3 PJ energy content of the fired household waste generated in the Budapest Waste Recovery Works (HuHa) and considering the energy efficiency of the facility, which is limited to 30 % [7].

The Budapest Waste Recovery Works is the only household waste-fired power plant in Hungary. Its task is to thermally dispose of about 60 % of household solid waste generated in Budapest. In 1976 a decision was made to set up a waste incinerator for a long-term solution of waste disposal with a capacity of 350 000 tons per year [8].

In the case of a major investment in energy utilization of household wastes, reducing natural gas dependence, increasing cost efficiency, increasing security of supply and optimizing the transport of heat and environmental sustainability, FŐTÁV has implemented a district heating connection between two major districts of the capital (North- Pest and Újpalota), thus enabling HuHa's annual capacity increase in heat production to be significantly increased and subsequently even doubled [7].

Because of the modernization, heat energy from the incineration of waste is used to heat water, so annual CO_2 emissions will be reduced by nearly 20 000 tonnes [9].

Networks and remote monitoring has a great added value in the operation of the system. FŐTÁV builds models for the simulation system from the performance data gathered in the monitoring system, which will support the enable of the planning of the co-operation.

Future plan is the construction of the (II.) Sewage Sludge and Waste Utilization Works and its connection to the district heating system of Budapest, which is suitable for the utilization of sewage sludge in household waste.

COMPLETE BUDAPEST HEAT COOPERATION AND ENERGETIC USE OF SEWAGE AND HOUSEHOLDS WASTE

Considering the expected savings, the investment cost and the expected heat turnover, the development of the comprehensive heating co-operation system in Budapest is a more significant development than the North-Western heat cooperation. Within the framework of the project, FŐTÁV intends to gradually develop the strategic connecting pipeline system in the capital. The resulting system will provide a high-utilized base load for the low-cost heat capacities of the heat producers currently operating or will be established in the future in the region (e.g. the new Sewage Sludge and Waste Utilization Works) [7].

The development would involve the joint utilization of household waste and sewage sludge, which would result in approximately 45-50 MW of waste-based combined heat and power generation capacities. Building a strategic pipeline and connecting the currently isolated areas is the criteria of the economical usage of this low-cost, 50 % renewable heat [10].

The creation of this system – like the North-Western heat cooperation and HuHa – reduces fossil energy dependency and contributes to the development of a sustainable environment. Among the goals of the strategic plan, it is important, that the interconnected Budapest system increases the competition of existing and engaging new heat sources, which improves the efficiency of supply. At the same time, the management of a much more complex system will move the operation control to smart network solutions.

INCLUSION OF FURTHER RENEWALS

In addition to communal waste, renewable energy sources in the district heating supply of the capital can be realistically utilized by combustion of solid biomass (mainly wood chips) and use of thermal water (limited in the deeper layers (2 000 m), so it is available for use in the primary district heating systems). Both power sources are included in the district heating contractor's plans for the medium term [7].

INVOLVEMENT OF HOUSEHOLD CONSUMERS TO REDUCE ENERGY CONSUMPTION

Given that in Hungary, 60 % of the energy consumption of buildings is provided by residential buildings [1], it is particularly important to address household consumers with information on energy saving and energy efficiency, and to encourage them to use less energy and use renewable energies.

The FŐTÁV has developed several plans to reduce household energy consumption and involve consumers in the process. One such application is the 'Okos-Ház' (*Smart-House* in Hungarian) project and another major development is the 'i love panel' project.

'OKOS-HÁZ' (SMART HOUSE) PROJECT

The aim of the tender announced for about 50 million Hungarian Forints, HUF (about 175 000 € at that time rate) in 2012 was to encourage consumer energy efficiency and energy saving. Further motives were promoting renewable electricity generation, since renewable heat production on the user side (eg solar collectors) is not a climate-effective solution, since it triggers the high efficiency cogeneration.

The residents of each building with district heating (condominium, housing co-operative) could apply the project, which was in the service area of FŐTÁV Zrt. and had a valid public utility contract with the service provider. Another condition was that only those buildings could be involved in the competition, in which the modernization of the secondary heating

system had already been completed and the installation of the thermostatic radiator valves had been completed in all the flats of the building. The conditions also included that the building's domestic hot water (DHW) circulation system should be fully built (extend to the riser pipes) and the building should have a lighting system in common areas [11].

Nearly fifty residential communities participated, and the four winner houses were partially modernized, with the total cost of the construction completed by FŐTÁV:

- modernization of the building's domestic hot water system: complete pipeline reconstruction, efficient thermal insulation, installation of the circulation system with thermostatic balancing valves,
- the full design of the "smart metering" system for both heating and DHW systems: installing cost-scaling devices in the heating system, incorporating electronically readable water meters and install a permanent read-out system in the building; retrieving the monthly measurement data to the billing system; publishing measurement data for user(s),
- electricity produced on solar panels can be used in the building-level accounting system, or if solar cells generate a yield that exceeds the current energy demand, it is fed back to the distribution system through a metering point transformed into a bi-directional energy measurement.

According to the primary calculations, upgrades can reduce energy consumption by up to 25 %: in the finished Smart Houses the results show, that 26 to 38% reduction in heat consumption, 6 % to 13 % in water consumption and 10 % in energy consumption were reached [12, 13].

'I LOVE PANEL' – THE MOST ECONOMICAL BUILDING

The competition announced by FŐTÁV in 2013 aimed also for promoting energy efficiency, energy saving and increasing renewable energy use among district heat users.

From the point of view of savings, heat, water and electricity consumption are of paramount importance, which are a key element of housing costs. The purpose of the 'I love panel project' was to compare the energy saving practices of buildings with these three factors and to find the most economical building built with industrialized technology [14].

Those buildings in Budapest could apply, which had been built with industrialized technologies; were equipped with district heating (both for the heating of buildings and for the heat source of domestic hot water production, with the latter having a fully developed circulation system); the modernization of the secondary (building) heating system had already been completed in the building; had a lighting system in common areas.

The winning buildings earned 1 kW of solar power with its respective inverters and fittings: the aim is to use solar panels to generate approximately 10 % of electricity consumption of the building in year.

The proposals were evaluated based on the above-mentioned three aspects: district heat, water and electricity consumption. Three evaluation features were identified for the comparison: district heat consumption (measured in GJ/m², kWh/m²); water consumption (measured in m³/m², l/m²) and saving of electricity (%).

Of the 13 entries received for the stringent requirements, the professional jury announced three winners: the energy value of the winners can serve as a guideline for other buildings - what are the goals to be pursued.

CONCLUSIONS

In Budapest, several major developments have been made in recent years regarding district heating (both on the producer side and with involving consumers), with the aim of efficient

energy management and the use of renewable energies, thus increasing overall environmental sustainability. The presented projects fit well into the smart city development strategy and emphasize the involvement of the household consumers and increase the consumer's energy awareness.

Among the presented projects, the 'Okos-Ház' (Smart House) project is an extensive and highly successful program. The success of the project is well exemplified by the fact that one of the winners in the project got a 2 kW solar panel, and then the community planted additional 15 kW at its own expense, multiplying its performance. Also within the framework of this project, the smart metering network, as well as automated cost distributors and scanners were installed and have been working properly, but the system has not encouraged consumers to make any further changes.

Projects show that there is great potential for consumer upgrades and consumer involvement. However, based on experience, consumers have no need to monitor their own consumption and change it. It is important in the future to stimulate consumers' awareness of energy: there are ways to measure energy consumption and track the results if consumers need it.

A development program does not in itself encourage the consumer community, to participate in such an action: any similar investment – with involvement of household consumers – will be successful if, on the one hand, consumers receive substantial financial support and a strong local endeavour. This is also the case with the projects presented: in communities where there was a local incentive force for investment, serious results could be achieved. However, to maintain serious results, it is necessary to reach these consumers.

The situation with the producer's side investments is different, they usually work as planned. System-level thermal co-operation works well in day-to-day operation, problems can be solved, objectives are met. The development points that further system operations are needed in order to increase the utilization of the given heat sources.

It is important for these developments to continue in the future and to increase the energy efficiency of district heating and to change the environmental awareness of communities together, reducing the burden of the built environment.

REFERENCES

[1] –: *National Building Energy Strategy.*
http://www.kormany.hu/download/d/85/40000/Nemzeti%20E%CC%81pu%CC%88letenergetikai%20Strate%CC%81gia%20150225.pdf, accessed 1st February 2018,

[2] Hungarian Statistical Office: *District heating and hot water supply (2000–).*
https://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_zrk008b.html, accessed 1st February 2018,

[3] Hungarian Statistical Office: *Housing stock and housing density, on 1st of January (2001–).*
https://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_wde003b.html, accessed 1st February 2018,

[4] Dobos, K., et. al.: *Smart City Knowledge Platform*. In Hungarian.
Lechner Tudásközpont, Budapest, 2015,

[5] Finta, S.; Barta, S. and Balogh Samu, M.: *Smart Budapest.*
Budapest 2024 Nonprofit Zrt., Budapest, 2017,

[6] –: *Smart City Knowledge Platform of Hungary*.
http://okosvaros.lechnerkozpont.hu/hu, accessed 19th January 2018,

[7] –: *Situation of district heating service in Budapest*.
http://www.fotav.hu/media/downloads/2017/02/20/7015.pdf, accessed 1st February 2018,

[8] –: *Waste Recovery Works.*
http://www.fkf.hu/portal/page/portal/fkfzrt/vallalatrol/letesitmeny/huha, accessed 10th February 2018,

[9] –: *FŐTÁV uses more energy from communal waste.*
http://www.fotav.hu/media/downloads/2017/02/20/6901.pdf, accessed 10th February 2018,

[10] Orbán, T. and Metzing, J.: *Creating a South-Budapest heat-engineering system*. Magyar Energetika **2014**(5), 16-19, 2014,
[11] –: *Okos-Házak project.* http://www.fotav.hu/palyazati-kiiras-2012-fotav-okos-hazak, accessed 1st February 2018,
[12] –: *Energy-saving data of OKOS-házak.* http://www.fotav.hu/hireink/fotav-okos-hazak/okos-hazak-megtakaritasi-adatai, accessed 1st February 2018,
[13] Okos-ház Project: *The maintenance costs of four residential communities are decreasing in Budapest.* http://onkormanyzat.mti.hu/hir/33510/okos-haz_projekt_negy_budapesti_lakokozosseg_rezsikoltsege_csokken_budapesten, accessed 10th February 2018,
[14] –: *I love panel project*. http://www.fotav.hu/i-love-panel, accessed 1st February 2018.

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