BUILDING AND OPERATING A SMART CITY

Richárd Pető[1], *and Dániel Tokody[2]

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

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

DOI: 10.7906/indecs.17.3.6
Regular article

Received: 7 February 2019.
Accepted: 31 August 2019.

ABSTRACT

Building and operating a smart city can only be based on solid foundations. However, such solid foundations – for example architectural, mechanical, IT, security, etc. factors – are unavailable or incomplete in most cases. Consequently, the process should begin with their design and construction. A construction site and its arrangement changes day by day. The building process of the structure of a building may be an important change, as, for example, after the substructure phase, the construction of a new level is completed in every two weeks, or after finishing the structure, the internal walls and the infrastructure of the building are added. These changes on the site, and the resources, needs, rules, and (work) processes necessary for such changes also keep changing. From the aspect of safety-science this means that new threats appear, the frequency of potential risks changes, and the extent of damage changes. The purpose of this article is to briefly describe the security issues relating to the building processes of smart cities, highlighting the field of information security.

KEY WORDS

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

CLASSIFICATION

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

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

INTRODUCTION

"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].

Therefore, the smart city is a city that uses data and technologies to improve the lives of its citizens and businesses. The key technologies behind the success of a smart city are the IoP (Internet of People) and the IoT (Internet of Things) [2].

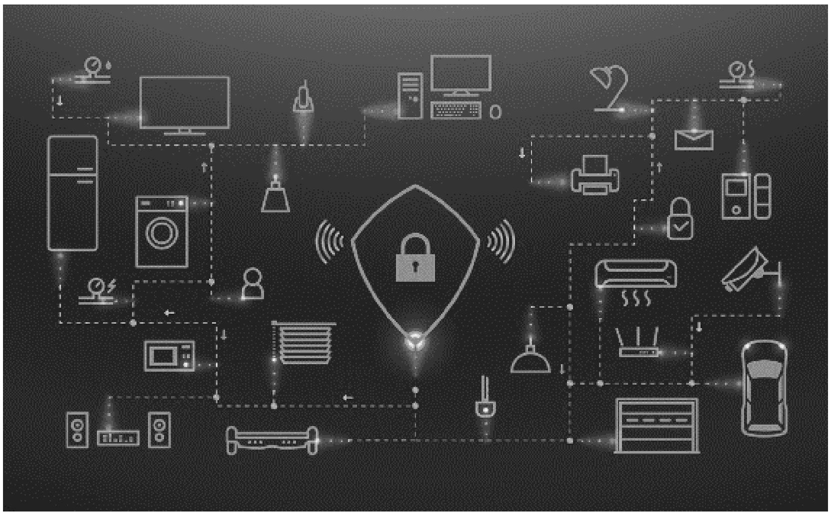

Figure 1. IoT devices [3].

The number of IoTs is well above that of the IoPs [4]. An increasing number of buildings, objects, or items are now equipped with some type of sensors (of light intensity, temperature, pressure, motion, or other physical, chemical, physiological impulses) [5]. Such sensors are the sensors of the IoT system, which are connected to the IoT platform through different networks and nodes.

The devices use these sensors to probe the environment from time to time (sound, air composition, visual images, etc.). The environment can be interpreted at several levels, such as a person or object, room, facility, settlement, etc. even globally.

Some specific examples are:

- a wrist watch that measures heart rate,
- a smart TV searching for voice prompts,
- an engineering control centre of a building, which adjusts the room temperature on the basis of human presence, set temperature and sun sensor data,
- an urban surveillance camera that records and transmits live images of people in public areas.

The signals reach the information processing site via (either wired or wireless) communication channels. The "size" of the data processing centre is fundamentally determined by the task assigned to it.

In China, a Social Credit System is planned to be introduced by 2020. The basic idea of the system is that the state can directly influence citizens by granting or denying certain activities based on the scores associated with the citizens' electronic profile. For example, people who have an insufficient amount of points, will be deprived of the chance to purchase a train or air ticket [6]. In March 2018, 9 million airline tickets and 3 million train tickets were blocked [7].

An interesting element of the system is that currently surveillance is supported by 200 million cameras in the country with nearly 1,4 billion inhabitants [8-10].

The centralised management of technological devices comprises a challenge in itself, not to mention the analytical and data management processes. In the beginning these resources are not available, they must be developed and operationalized [11, 12].

Unfortunately, for the past several years in the construction industry, I have not experienced any development in the field of security technology (and IT protection in particular) in large-scale (and small-scale) construction projects. One possible reason for this may be that the construction sector has an extremely high percentage of undeclared work force: "According to the Labour Inspectorate of the National Tax and Customs Administration (NAV), in the first three quarters of 2015, the construction sector had the highest level of undeclared work force – nearly 3 300 inspections were carried out in construction companies, and more than two-thirds of them were found to have some irregularities. Undeclared work means employment bypassing labour and tax regulations and other employment legislations" [13].

The following chapters will briefly review, in general terms, the security problems encountered during construction processes.

PARTICIPANTS OF A CONSTRUCTION PROJECT

This chapter describes the actors involved in the construction process and their roles, as well as the organizational plan process, which is important for implementation and, at the same time, for safety technology.

THE CUSTOMER

The customer identifies the investment to be realized. (S)he signs a contract with a general contractor on the construction, acquires building permissions, monitors the construction work, covers the costs of building and later those of maintaining the facility, etc. The necessary expenses are covered from own resources or from a bank loan [14].

THE GENERAL CONTRACTOR

The general contractor enters into an obligation to carry out construction and technology work in a comprehensive manner. The general contractor's scope of responsibilities includes "assembly preparation work (fence building around the construction site, constructing electrical transformers and measuring points, installing site buildings, constructing temporary roads); civil engineering work (excavation, building foundations, substructures, public utilities and doing ancillary work); overground construction work (supporting structures, partitioning structures, cladding and finishing work, interior decoration, installation of doors and windows and their ancillary work); building engineering (installation of water and gas supply systems and sewerage, lifts, installation of central heating, electrical fittings, building installation and fitting work and their ancillaries); withdrawal and follow-up work, and contracting (with the customer in the case of a general contractor, or with the general contractor in the case of subcontractors. The task of the general contractor is to select subcontractors, suppliers, service providers involved in the implementation and contracting through direct calls for tenders), to complete implementation in accordance with the terms of the contract, to perform trial runs with the completion of additional work as required, to report to the customer, to hand over the facilities during the procedure (with the delivery of handover documentation and other necessary documents to the customer), and to fulfil the warranty obligation" [14; pp.6-7].

SUBCONTRACTORS

Their task is to fulfil the contract with the general contractor. Their activities may be described as "identical" at all construction sites, and are generally considered as professional activities [15], such as determining basic qualitative and quantitative data for construction work, material storage – transportation – loading and foundation, constructing supporting structures and partition walls, electrical- water- and gas-supply networks, building distribution systems, performing service activities, providing electrical and electronic systems, preparing a construction schedule (human resources, mechanization, workflows, technologies, finances), facade scaffolding, guarding, performing technical inspection activities and developing IT and telecommunications systems.

THE CONSTRUCTION YARD

THE ORGANIZATION PLAN

The coordination of tasks over time and space is achieved through a so-called organizational plan, which contains all the technical elements necessary to carry out the construction. There may be several organizational plans depending on the stage of the investment that is in progress [15, 16]. According to these stages a distinction may be made between an organizational map, organizational outlines, a detailed organizational plan, a general organizational layout plan, an organizational status plan, a workflow layout plan, and technological blueprints.

The plans listed above include information on the geographical location of the construction site, the location of the elements that will serve the construction site within the specific construction site. Such temporary or permanent elements [15] may comprise, for example, access routes, road construction opportunities, cable networks and pipelines of water, gas, electric power supply, the boundary of the facility under construction, positions of machinery (e.g. tower cranes), disposal areas, access areas, locations of ancillary facilities, etc.

An organizational plan is important from a data protection point of view, as it contains confidential information about the structure of the construction to be built and the design of the construction site.

SAFETY AND SECURITY SYSTEMS

In general, safety and security includes the following areas:

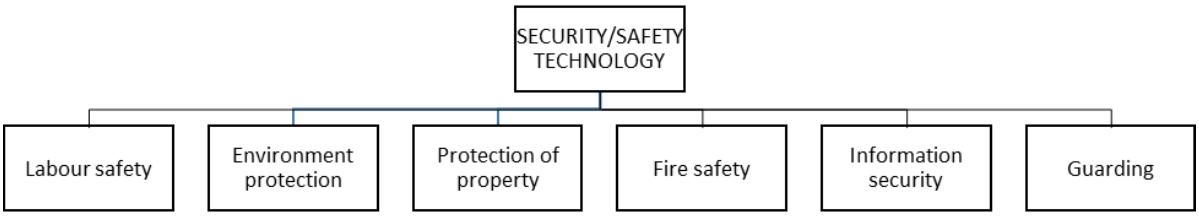

Figure 2. Areas of security technology.

On the basis of their function, the six branches above may be divided into two sections. One of them is occupational safety, fire safety and environmental protection, which is usually abbreviated as EHS or HSE (Environment – Health and Safety). Their primary role is to prevent and manage personal injuries, property and environmental damage which are consequences of accidents related to work [17; p.87 §1/A].

The other group is "Security", which includes property protection, information protection and guarding. The primary purpose is to prevent, pre-empt or protect against intentional damage and injuries.

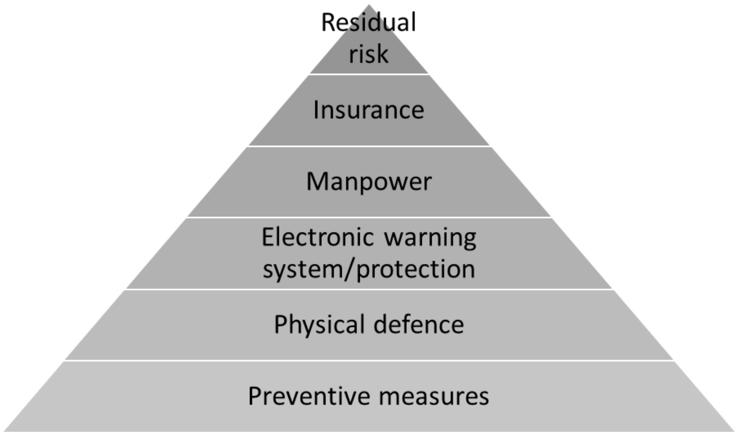

Figure 3. Steps of establishing security/safety (Security Pyramid) [18; p.13].

The development of the protection concept is based on risk assessment and evaluation. The security pyramid illustrates the components of protection and how they are built on one another. Each level has its own "mission". Each level can be further divided into sub-levels or components, which may be called efficient, depending on how they have met the criteria.

Of all the sub-sectors, the present article deals with the information security sector. The figure below shows that there are five major subsectors, some of which are also present within the security technology sector. The dual appearance can be explained by the difference between the primary objectives and the specificity of the trade.

Requirements towards the areas of implementation are primarily determined by legislation and a further regulator called corporate management security policy (hereinafter referred to as management policy).

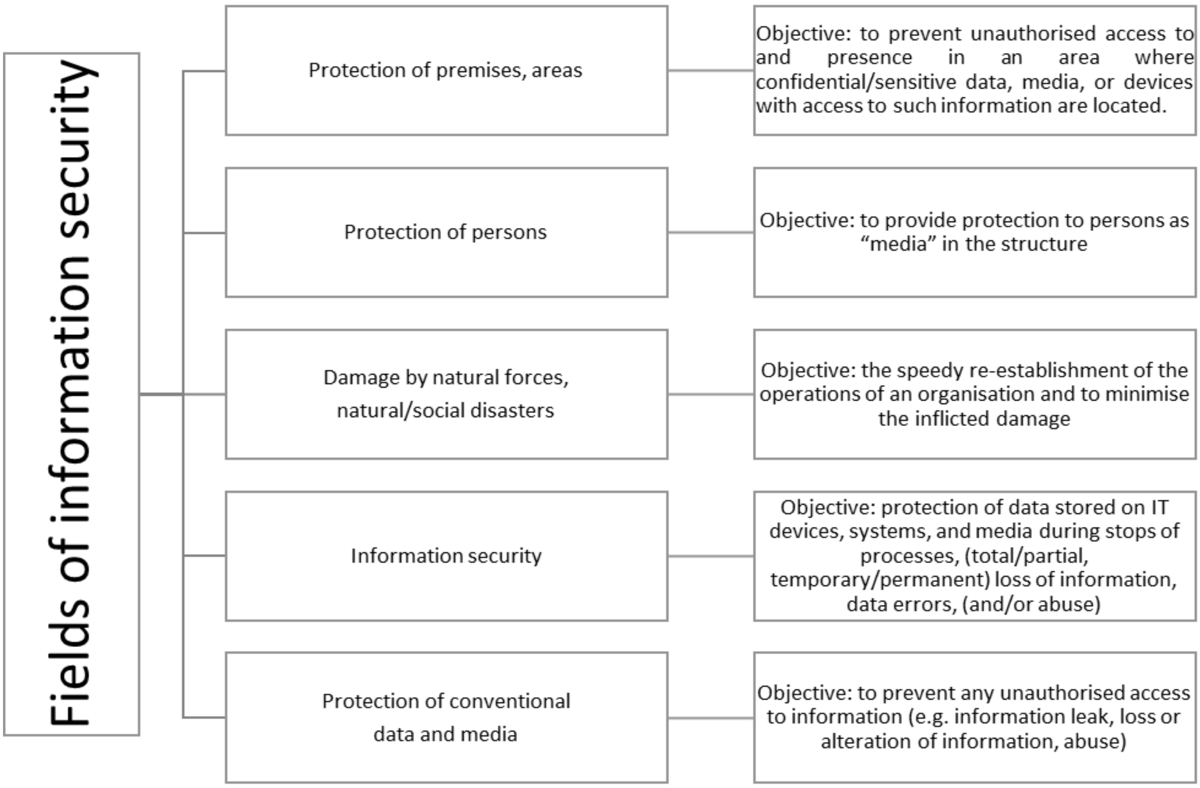

Figure 4. Areas for implementing information protection procedures [19].

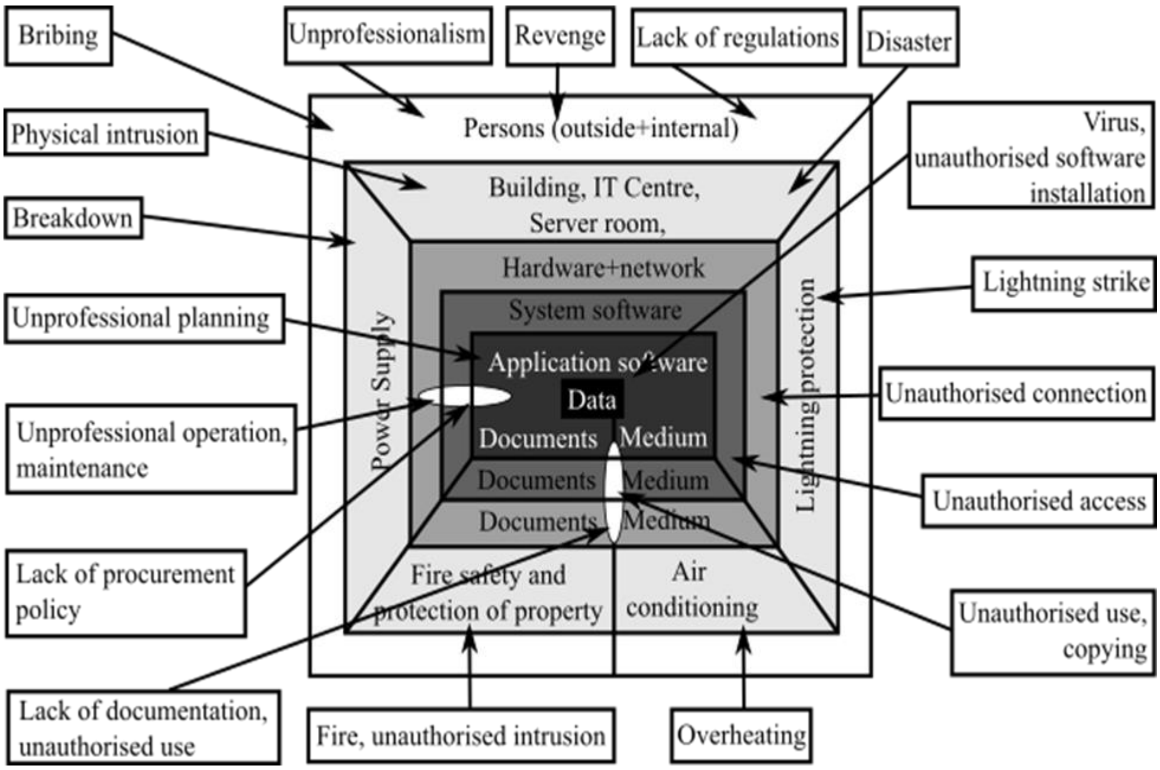

Figure 5. Example of grouping threats [20; p.33].

INFORMATION SECURITY

The primary purpose of information security is to preserve the integrity, confidentiality, availability, authenticity, accountability, non-repudiation and reliability of data (information) against threats.

Information in the field of constructions may include, for example:

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

The previous description and the Table 6 illustrate only a small fraction of the problems that may occur. A wrong decision associated with the construction process or data management may generate huge additional costs (liquidated damages, fines: see GDPR regulation) [24].

Table 6. A few examples of practical risk assessment.

Responsible person: Subcontractor	**Identification of risk – potential harmful events**		
Guard office and checkpoints	**Description of frequent mistakes or dangers**	**Primary impact of risks**	**Secondary impact of risks**
1.	Number and range of vision of CCTV cameras are compromised	Leaking classified information, potential analysis of the security scheme of construction site	▪ Material damage, ~ increase of costs (theft, deterioration, etc.)
2.	Operability of CCTV cameras is compromised	Leaking classified information, potential analysis of the security plan of construction site	▪ Material damage, ~ increase of costs (theft, deterioration, etc.)
3.	Paper-based media are accessible for unauthorized persons	Leaking classified business data, in dependence on their type	▪ Delay of construction processes (waste of time) ▪ Additional expenses
			▪ Penalties and fines
			▪ Uncertain results in construction and other undertakings
4.	Stored keys are accessible for unauthorized persons	Intrusion of unauthorized person into the construction site	▪ Material damage, ~ increase of costs (theft, deterioration, etc.)
		Leaking classified business data, in dependence on their type	▪ Uncertain results in construction and other undertakings
			▪ Penalties and fines
		Leaking classified information, potential of analysis of the security plan of construction site	▪ Material damage, ~ increase of costs (theft, deterioration, etc.)

CONCLUSION

Apparently a smart city is an extremely complex IT system based on information sharing, its accessibility and accuracy. The construction of the system – or the network (eg. critical information infrastructures) – involves numerous processes. These are also based on a multitude of data requests and data management, which means the use of databases which also need to be addressed. At the moment, the difference between a system under construction and a completed operating system is that the latter can provide much more information and it works faster. The real question is, however, that, before launch and operation, who will have access to confidential information and for what purpose will they intend to use such information [25, 26].

REFERENCES

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

[2] National League of Cities: *Trend sins smart city development*. https://eu-smartcities.eu/sites/default/files/2017-09/Trends%20in%20Smart%20City%20Development.pdf, accessed 29th May, 2018,

[3] Pic.: *IoT devices*. https://s28241.pcdn.co/wp-content/uploads/2018/02/IoT-Security-blog-banner.jpg, accessed 28th July 2018,

[4] Bakonyi, P., et al.: *Az okos város (Smart City)*. Nordex Nonprofit Kft. – Dialóg Campus Kiadó, Budapest, 2018,

[5] Heuser, L.: *International Smart City plans, experiences, success factors*. Híradástechnika **73**(1), 2-9, 2018,

[6] Matthew, C.: *Leave no dark corner*. https://mobile.abc.net.au/news/2018-09-18/chinasocial-credit-a-model-citizen-in-a-digital-dictatorship/10200278?pfmredir=sm,

[7] Creemers, R.: *China's Social Credit System: An Evolving Practice of Control*. SSRN, 1-32, 2018, http://dx.doi.org/10.2139/ssrn.3175792,

[8] Udemans, C.: *Blacklists and redlists: How China's Social Credit System actually works*. https://technode.com/2018/10/23/china-social-credit,

[9] HVG: *Egy durva bemutató: Így működik Kínában a mindent megfigyelő, mindenről tudó rendszer*. https://hvg.hu/tudomany/20180919_kina_tarsadalmi_kreditrendszer_hogyan_mukodik_pontszam_megfigyeles_digitalis_diktatura,

[10] Kovács, T. and Miklós, G.: *A biometrikus adatok kezelésének jogi szabályozása*. Hadmérnök **14**(1), 8-16, 2019,

[11] –: 252/2018. (XII. 17.) *Korm. rendelet az okos város központi platformszolgáltatás létrehozásáról és működtetéséről*. https://net.jogtar.hu/jogszabaly?docid=A1800252.KOR,

[12] –: 314/2012. (XI. 8.) *Korm. rendelet a településfejlesztési koncepcióról, az integrált településfejlesztési stratégiáról és a településrendezési eszközökről, valamint egyes településrendezési sajátos jogintézményekről*. https://net.jogtar.hu/jogszabaly?docid=a1200314.kor,

[13] Wéber, L.: *A feketemunka az építőipar változatlan problémája*. http://www.terc.hu/cikk/a-feketemunka-az-epitoipar-valtozatlan-problemaja,

[14] Lovas, A.: *Építéskivitelezési Tanulmány – Palántaház Tehetségkutató Központ Győr*. Budapesti Műszaki És Gazdaságtudományi Egyetem Építéskivitelezési Tanszék, Budapest, 2010,

[15] Építővilág: *Organizációs terv*. http://epitovilag.hu/organizacios-terv, accessed 17th May, 2018,

[16] Gombosné Rása, É.: *Az építőipari kivitelezési munkák előkészítése*. http://www.kepzesevolucioja.hu/dmdocuments/4ap/9_0459_tartalomelem_001_munkaanyag_100228.pdf, accessed 23rd May, 2018,

[17] –: *1993. évi XCIII. törvény a munkavédelemről*. https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=9, accessed 14th February 2018,

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

[19] Horváth, Zs.: *Bevezetés az információbiztonságba*. Óbudai Egyetem, Budapest, 2017,

[20] Horváth, Zs.: *Az információbiztonsági irányítási rendszer alapjai*. https://anzdoc.com/az-informaciobiztonsagi-iranyitasi-rendszer-alapjai.html, accessed 14th December 2018,
[21] –: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. https://net.jogtar.hu/jogszabaly?docid=a1100112.tv, accessed 24th May, 2018,
[22] Constructible: *Cybersecurity In Construction: What You Need to Know*. https://constructible.trimble.com/construction-industry/cybersecurity-in-construction-what-you-need-to-know,
[23] MyIT: *3 Biggest Construction Cybersecurity Risks*. https://www.myitsupport.com/blog/construction-cybersecurity-risks,
[24] CIOB: *The role of security in the construction industry*. https://www.ciob.org/sites/default/files/The_Role_of_Security_in_the_Construction_Industry.pdf,
[25] Illési, Z.; Halász, A. and Varga, P.J.: *Wireless Networks and Critical Information Infrastructure.* 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, 2018,
2016 IEEE 17th International Symposium on Computational Intelligence and Informatics. IEEE, Budapest, 2016,
http://dx.doi.org/10.1109/SACI.2018.8441023,
[26] Varga, P.J.: *A kritikus információs infrastruktúrák értelmezése.* Hadmérnök **3**(2), 149-156, 2008.