17(3-A), pp.430-519, 2019 **ISSN 1334-4684**

INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS

Scientific Journal

Scientific Journal
INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS

INDECS, volume 17, issue 3, part A, pages 430-519, year 2019
Published 30th September 2019 in Zagreb, Croatia
Released online 30th September 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 week before the publishing date.

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

TABLE OF CONTENTS

REGULAR ARTICLES

COMPLEX SYSTEMS AND SMART CITIES RESEARCH. EDITORIAL

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

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

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

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

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

Cordially,

Budapest, 31st August 2019

Guest editors:

Dániel Tokody

Gyula Mester

Interdisciplinary Description of Complex Systems 17(3-A), 430-437, 2019

LEARNING PLATFORM FOR SMART CITY APPLICATION DEVELOPMENT

Dalibor Dobrilović[1,] *, Milan Malić[2] and Dušan Malić[3]

[1]University of Novi Sad, Technical Faculty "Mihajlo Pupin"
Zrenjanin, Serbia

[2]Panonit
Novi Sad, Serbia

[3]Technical College of Applied Sciences in Zrenjanin
Zrenjanin, Serbia

DOI: 10.7906/indecs.17.3.1
Regular article

Received: 30 November 2018.
Accepted: 31 August 2019.

ABSTRACT

With the emerging trend of the Internet of Things and Smart City environments, new trends have arisen in building applications, too. The current approach to application development, known as monolithic architecture, is not suitable for the newest appliances. Recently, the microservice-based application architecture has emerged as a potential solution that could meet the imposed challenges. In order to educate new generations of software and IT engineers to be able to develop such microservice-based applications, educators at universities should establish an efficient platform to ensure this process. This article presents the portable and lightweight platform for teaching application development based on microservices. The platform is focused on supporting lightweight publish/subscribe messaging protocols, such as MQTT, and built-on open-source hardware development boards such as Arduino/Genuino. This Smart City learning platform is designed to enable the collaborative development of systems, applications and services for the cities of the future, and it should be efficient enough to support the learning of all the necessary skills that can be used for the development of complex and large-scale systems. The architecture of the proposed platform, as well as its elements are presented in this article.

KEY WORDS

smart city services, engineering education, publish-subscribe protocols, microservices, IoT

CLASSIFICATION

ACM: 10011007.10010940.10010971.10010972.10010975
JEL: L86
PACS: 07.07.Df; 07.05.Bx

*Corresponding author, η: dalibor.dobrilovic@uns.ac.rs; ++381 62 8019760;
Technical Faculty "Mihajlo Pupin", Djure Djakovica bb, 23 000 Zrenjanin, Serbia

INTRODUCTION

The variety of the software and hardware technologies that have appeared in the past decade has shaped new trends for the ICT market. With novel trends, such as the Internet of Things and Smart City environments, new solutions for building applications have emerged as well. The current approach of monolithic architecture development is not suitable for the appliances in these new environments. In order to meet the imposed challenges, the architecture of microservice-based systems has arisen as a potential solution. The capability of higher education institutions to educate new software and IT engineers for the development of microservice-based applications has become an important issue. In order to address this challenge, universities should establish an effective learning platform for such process.

This article presents the portable and lightweight platform for teaching microservice application development. The platform is based on open-source hardware and software and it is focused on supporting lightweight publish/subscribe messaging protocols such as MQTT. Open-source hardware development boards such as Arduino/Genuino and clones are used as devices for the platform. The Smart city learning platform is planned to be used in the learning process within university curricula and it is designed to enable the collaborative development of systems, applications and services for the smart cities of the future.

RELATED WORK

The importance of integrating microservice-based application development in engineering education, especially in IoT and Smart City environments, has been underlined by the following references. According to the first paper, the microservice architecture has emerged to meet the industry's needs for scalability, evolvability and maintainability of large-scale distributed systems. Also, microservices have received a wide adoption in the industry among companies building large-scale applications, such as Amazon and Netflix, as well as Platform-as-a-Service (PaaS) providers, such as Pivotal [1]. At the same time, the authors shared their early experience in applying the microservice architectural style to build a Smart City IoT platform for a variety of applications.

In the second paper [2] the authors present a microservice-based architecture equipped with a real-time environmental sensor system that has highly scalable applications in a cloud environment. The purpose of the proposed system is to monitor and control the transportation of hazardous materials. The authors integrated the global positioning system (GPS) technology, wireless sensor networks (WSN), geographic information system (GIS), in addition to IoT technologies, to achieve real-time monitoring and tracking of hazardous materials.

The use of a microservice architecture designed to address the key practical challenges in smart city platforms called InterSCity is presented in another paper [3]. This is a microservice-based, open-source, smart city platform that enables the collaborative development of large-scale systems, applications and services for the cities of the future, contributing to turn them into truly smart cyber–physical environments [4]. The platform is presented together with the set of experiments that evaluate its scalability [5].

This article presents the platform for teaching microservice application development based on open-source hardware and software. The main motivation for developing the presented platform was to enable the teaching of application development based on a group of protocols. This group of protocols can be called application layer protocols, although different names such as messaging protocols, publishing-subscribe protocols or machine-to-machine protocols can be used as well. This group includes protocols such as MQTT

(Message Queuing Telemetry Transport), AMQP (Advanced Message Queuing Protocol), XMPP (Extensible Messaging and Presence Protocol), DDS (Data Distribution Service), HTTP (Hypertext Transfer Protocol) and CoAP (Constrained Application Protocol) [6]. They are widely used in Smart City systems, and, as an example, the comparison of the response time of communication protocols such as CoAP, MQTT, XMPP and WebSocket, used in smart parking system is given in [7].

The platform has inspired similar studies [8-11] and the previous works of the authors of this article [13], with a focus on supporting lightweight publish/subscribe messaging protocols such as MQTT [11, 12]. The platform is built on open-source hardware development boards such as Arduino/Genuino. This Smart City learning platform is designed to enable the collaborative development of systems, applications and services for the cities of the future, and it should be efficient enough to support the learning of all the necessary skills required for the development of complex and large-scale systems. The architecture of the proposed platform (hardware and software components of the learning system) as well the experience with its usage, are presented in this article.

HARDWARE COMPONENTS OF THE LEARNING PLATFORM

Figure 1 shows the scheme of the learning system called LearnMQ. The system has six hardware components. These components include a laptop, an access point and three sensor nodes. All devices in the system support the IEEE 802.11 technology for networking. The laptop has a built-in wireless interface, and the other devices use ESP8266 communication modules. The function of the hardware components is described in this section.

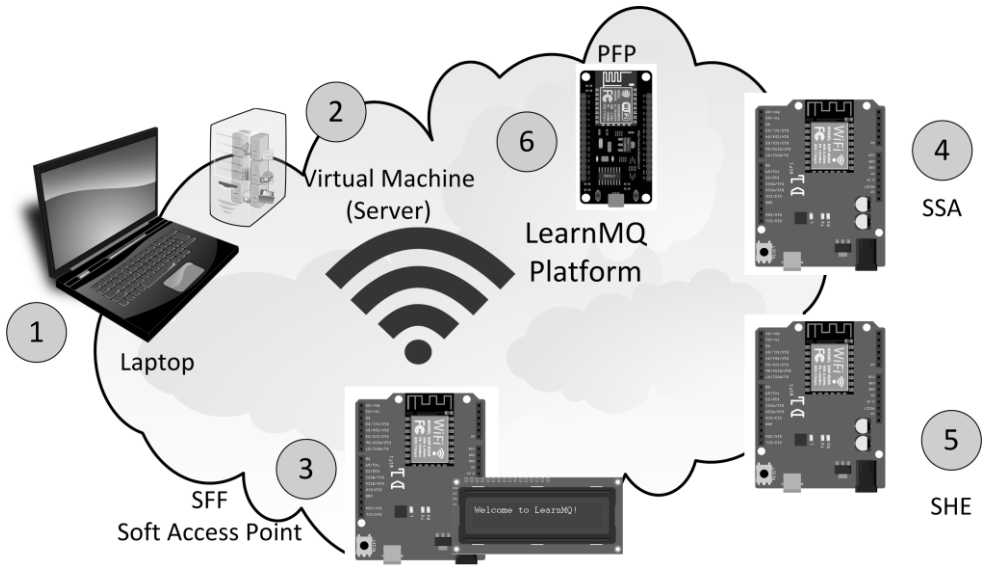

Figure 1. The topology of the learning system.

The first system component is a laptop (1). The laptop has Windows 10 operating system and the following software installed: Oracle VM virtual box as virtualization software, Python 3.6 for application development and Wireshark as the network traffic analysing software. The role of this device is to be one of the wireless clients in the network, and to host Python publishing and subscribe applications. The laptop also hosts an SQLite database for sensor data storage. The second component installed on the same device is a virtual machine (2). This is a CentOS 7.4 server with Mosquitto broker installed. It has the role of a publish/subscribe broker server. The virtual machine uses virtual Wi-Fi interface in bridged mode with fixed IP address 192.168.100.100 needed for the Mosquitto MQTT broker. All the other devices use dynamically allocated IP addresses assigned by the access point (3). The

utilization of the Wi-Fi interface is essential for this platform since that interface is used for transferring the data from all sensor nodes to the MQTT broker and subscriber application. The same interface is used for analysing the network traffic with Wireshark.

The third component (3) is designed as an access point. It is an Arduino/Genuino UNO clone with an integrated ESP8266 communication module called Wemos D1 R2. This module enables communication by using the IEEE 802.11 technology. This device is designed to have the role of the access point. In order to provide the feedback information for users, the I2C LCD 20x4 is attached to it. Its role is to act as the access point in the wireless network and to allow connection for other wireless clients. This device also has the role of a DHCP server.

The devices (1), (4), (5) and (6) use the access point to connect to the network. The LCD is used to show the number of devices connected to the network, and the information that can be used for other client devices to access the network, such as the network name (SSID) and passphrase. The IP address of the access point (192.168.100.2) is displayed as well. The problem with the usage of Wemos D1 R2 or any similar device based on ESP8266 as the access point is that there is a limitation to connecting up to four wireless clients. The default setting of the device is limited to four clients, although, according to the documentation, there is a possibility to extend this limitation up to eight devices. For the present research, the authors did not make a change to increase the limit of connected devices. As an alternative, an Android smartphone as a Wi-Fi hotspot can be used. The Android smartphone also has a limitation of allowing up to eight connected devices per network. The second alternative is to use the real access point as a dedicated device or a device that is part of the infrastructure. In order to make this learning platform easy to set up and portable, the Wemos D1 R2 or Android smartphone is considered for usage. For this particular research, only the Wemos D1 R2 is used. The laptop with a Python publishing script simulates the fourth sensor node with stationID TIS. The laptop does not have a sensor attached to it, and the sensor values are generated randomly.

Three devices (4), (5) and (6) represent wireless sensor nodes. They are built on Arduino/UNO clone devices. Each device is built upon a different clone type. The node with stationID SSA is based on Wemos D1 R2 (4), the node with stationID SHE (5) is based on Espduino and the node with stationID PFP (6) is based on NodeMCU. Each node has an attached gas sensor MQ-135 for air quality monitoring. The sensors are not calibrated, and sensor accuracy is not important in this case. These sensors are used to generate data to be transferred (published) to the message broker. The devices use MQTT protocol for publishing sensor data. The Arduino IDE is used for device programming with the usage of additional MQTT library. All three devices can be programmed using the same IDE code (with minor changes) and libraries.

SOFTWARE COMPONENTS OF THE LEARNING PLATFORM

The software architecture of the system is based on the microservices model, and it is presented in Figure 2. The figure describes six main software components of the learning platform. The first presented component of the system (1) is the MQTT broker. The Mosquitto software is used as the MQTT broker. It is installed on the previously described CentOS server, deployed on the virtual machine. The Mosquitto server listens to port 1883 for accepting publishing messages. All messages containing sensor data and additional information are sent using the MQTT protocol and are directed to my_queue.

The sensor nodes (2), (4), (5) and (6) send sensor data via the MQTT protocol to the Mosquitto broker. First node (2) uses Python script to simulate sensor data. The other three nodes (Arduino/Genuino UNO clones) are prototyped wireless sensor stations that send gas

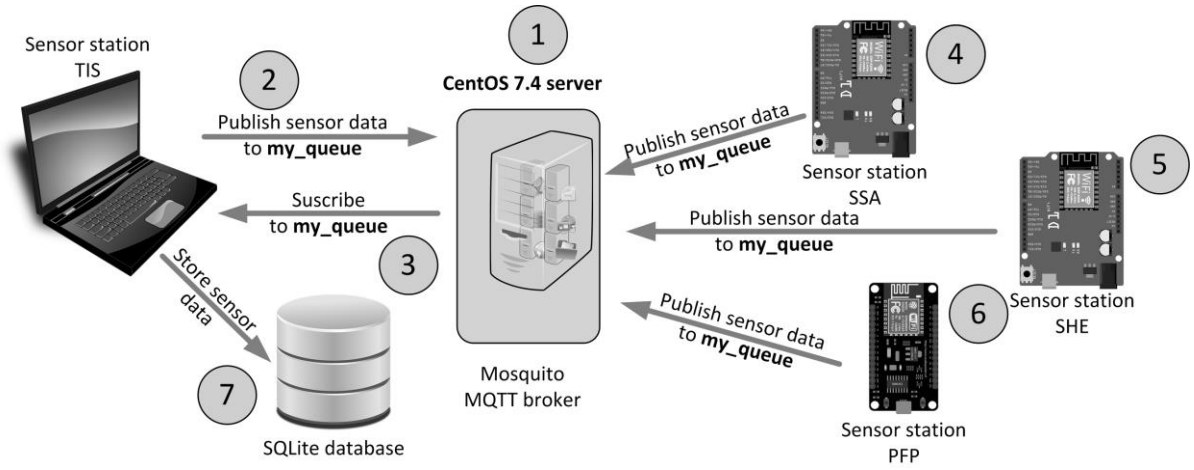

Figure 2. The architecture of the learning system.

sensor data. Data acquisition is enabled by a non-calibrated MQ-135 gas sensor designed for air quality monitoring. Since the purpose of the presented platform is not environment monitoring in real systems, the sensor data are sent in raw format. The value of the data ranges from 0 to 1023 and represents an analogue value read with the Arduino function analogRead(). All nodes have a stationID consisting of three letters. The three nodes have following IDs respectively: SSA, SHE and PFP. The laptop has stationID TIS. All four nodes send the data in CSV format. The message begins with the stationID, followed by a comma and the sensor value, e.g., DHE,748. In this research no particular attention is paid to define the format of the message. So the message length is 8 bytes. Three bytes are used for the stationID, one byte for comma, and four bytes for sensor values. The MQTT message has a total length of 16 bytes, 8 bytes for sensor node data with the addition of 8 bytes for the name of the queue (my_queue).

The software component (3) is a Python script that enables subscription to the MQTT broker and the data sent to my_queue. Besides the subscription to the sensor data published in my_queue, the script displays the received messages on a computer screen and stores the received data in an SQLite database (7). The SQLite database is used in this architecture because of its simplicity, but for the future usage, document-oriented database systems such as MongoDB or time series database (TSDB) such as InfluxDB will be considered.

EXPERIENCES WITH THE PLATFORM

The platform has not yet been validated in the teaching process. However, platform validation was carried out in the testing phase with experimental runs. During these experimental runs, the platform proved to be stable and worked without problems. The platform is easy to set up, and the devices connect in the ad-hoc wireless network without a problem. After powering on all devices, the platform starts to work automatically, since the Mosquitto broker runs automatically on server start, and sensor nodes automatically attempt to assign to the Mosquitto broker. After successful assignment to the broker, each sensor node immediately starts to send sensor data in five-second intervals. The example of messages received with the subscription script is displayed on the laptop screen in the corresponding form (Figure 3).

Traffic analyses, which can be used to teach students the main principles of publish/subscribe protocols, and network data analyses are performed with Wireshark – widely used network analyzing software. Wireshark has supported the MQTT protocol since version 1.12.0. The platform in operating mode during the testing period is presented in Figure 4.

```
Received message: TIS, 392
Received message: SHE, 214
Received message: TIS, 990
Received message: SSA, 350
Received message: PFP, 528
Received message: TIS, 990
Received message: TIS, 987
Received message: SHE, 222
Received message: SSA, 272
Received message: PFP, 515
 Received message: TIS, 85
```

Figure 3. Received messages displayed by the subscriber.

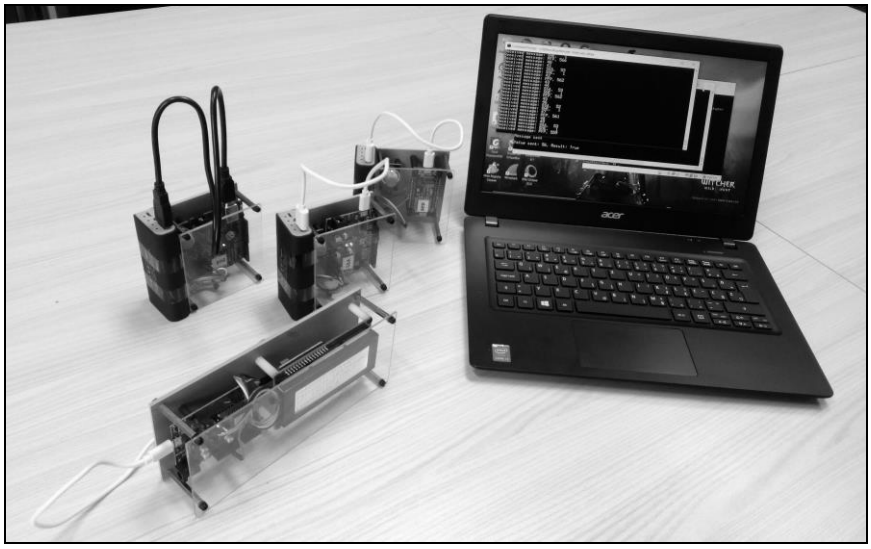

Figure 4. The learning system in testing period.

The platform was in test usage four times for about five hours. During this period, the platform worked without any problems. Based on the operation of the platform during the testing phase, it can be concluded that the platform is stable and it works correctly. Regarding the easiness of using the platform, it was concluded that the platform is suitable for usage in the classroom, for demonstrating the functioning of publishing/subscribe protocols, as well as for the students' collaborative work on the development of microservice-based applications.

CONCLUSION

This article presents a portable and lightweight learning platform for teaching IoT or publishing/subscribe protocols. This platform is focused on teaching and explaining the main principles of the the MQTT protocol, but it can be expanded with other similar protocols as well (AMQP, XMPP, etc.). The platform is designed to be used in the engineering education process within university curricula in order to enable the students to learn IoT technologies. This platform can be used for teaching microservice-based application development for the IoT. The presented platform is entirely based on open-source hardware and software, which makes this platform low-cost and easily applicable.

Further research will be conducted in three principal directions. The first direction is the expansion of this platform in order to support a more extensive range of protocols, primarily the AMQP (with server such as RabitMQ) and XMPP (with server such as Prosody). The usage of other databases such as MongoDB and InfluxDB will also be also considered. In order to use the platform in the learning process, educational materials and tutorials should be provided. The lack of tutorials is one of the main reasons why the platform has not yet been

evaluated in the learning process. After the completion of the tutorials and the design of laboratory exercises, the next step will be the experimental usage of the platform in the learning process. Finally, an effort will be made to adopt this platform to be used as a testing model for real-world IoT application development.

ACKNOWLEDGMENT

This research is supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia under the project number TR32044 "The development of software tools for business process analysis and improvement" 2011-2019.

REFERENCES

[1] Krylovskiy, A.; Jahn, M. and Patti, E.: *Designing a Smart City Internet of Things Platform with Microservice Architecture*.
Proceedings of 3rd International Conference on Future Internet of Things and Cloud. IEEE, Rome, 2015,
http://dx.doi.org/10.1109/FiCloud.2015.55,

[2] Cherradi, G.; EL Bouziri, A. and Boulmakoul, A.; Zeitouni, K.: *Real-Time Microservices Based Environmental Sensors System for Hazmat Transportation Networks Monitoring*.
Transportation Research Procedia **27**, 873-880, 2017,
http://dx.doi.org/10.1016/j.trpro.2017.12.087,

[3] Del Esposte, A.M.; Kon, F.; Costa, F.M. and Lago, N.: *InterSCity: A Scalable Microservice-based Open Source Platform for Smart Cities*.
Proceedings of the 6th International Conference on Smart Cities and Green ICT Systems. Science and Technology Publications, Lda, Porto, 2017,
http://dx.doi.org/10.5220/0006306200350046,

[4] Flammini, F.: *Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction.*
Springer, Cham, 2019,
http://dx.doi.org/10.1007/978-3-319-95597-1,

[5] Del Espostea, A.M., et al.: *Design and evaluation of a scalable smart city software platform with large-scale simulations.*
Future Generation Computer Systems **93,** 427-441, 2018,
http://dx.doi.org/10.1016/j.future.2018.10.026,

[6] Dizdarević, J.; Carpio, F.; Jukan, A. and Masip-Bruin, X.: *A Survey of Communication Protocols for Internet-of-Things and Related Challenges of Fog and Cloud Computing Integration.*
ACM Computing Surveys **51**(1), No. 116, 2019,
http://dx.doi.org/10.1145/3292674,

[7] Kayal, P. and Perros, H.: *A comparison of IoT application layer protocols through a smart parking implementation*.
20th Conference on Innovations in Clouds, Internet and Networks (ICIN). IEEE, Paris, 2017,
http://dx.doi.org/10.1109/ICIN.2017.7899436,

[8] Kashyap, M.; Sharma, V. and Gupta, N.: *Taking MQTT and NodeMcu to IOT: Communication in Internet of Things.*
Procedia Computer Science **132**, 1611-1618, 2018,
http://dx.doi.org/10.1016/j.procs.2018.05.126,

[9] Barbon, G.; Margolis, M.; Palumbo, F.; Raimondi, F. and Weldin, N.: *Taking Arduino to the Internet of Things: The ASIP programming model*.
Computer Communications **89-90**, 128-140, 2016,
http://dx.doi.org/10.1016/j.comcom.2016.03.016,

[10] Prada, M.A., et al.: *Communication with resource-constrained devices through MQTT for control education*.
IFAC-PapersOnLine **49(**6), 150-155, 2016,
http://dx.doi.org/10.1016/j.ifacol.2016.07.169,

[11] Komkrit Chooruang, K. and Mangkalakeeree, P.: *Wireless Heart Rate Monitoring System Using MQTT*.
Procedia Computer Science **86**, 160-163, 2016,
http://dx.doi.org/10.1016/j.procs.2016.05.045,

[12] Hillar, G.C.: *MQTT Essentials – A Lightweight IoT Protocol*.
Packt Publishing Ltd., Birmingham, 2017,

[13] Malić, M.; Dobrilović, D. and Malić, D.: *Predlog arhitekture sistema za podršku bežičnim senzorskim mrežama zasnovanog na mikroservisima*. In Serbian.
XXXVI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju. Beograd, 2018.

Interdisciplinary Description of Complex Systems 17(3-A), 438-443, 2019

THE ROLE OF ADDITIONAL INFORMATION IN OBTAINING INFORMATION

Edina Albininé Budavári* and Zoltán Rajnai

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

DOI: 10.7906/indecs.17.3.2
Regular article

Received: 30 December 2018.
Accepted: 31 August 2019.

ABSTRACT

One of the basic components of the smart city concept is the infocommunication infrastructure. The purpose of the infocommunication system is, among others, to transmit information. Generally, besides the necessary information provided in a transmission, some additional information is displayed as well. In public communication the destination of the information is not a specific person or object. Therefore, additional information can be obtained by anyone. Thus, such additional information facilitates the unwanted acquisition of information and its later use. The present study illustrates the role of additional information in obtaining information through an example of an online game. This game is public, therefore, it is an open source of information. The technology of Open Source Intelligence is one of the basic elements of the social engineering information palette.

KEY WORDS

additional information, open source, obtain, OSINT, social engineering

CLASSIFICATION

ACM: J.4, K.4
APA: 4010
JEL: D83

*Corresponding author, η: abepubkut@gmail.com; +36 20 425 4605;
OE-BDI office, Nepszinhaz str. 8, 1081 Budapest, Hungary

INTRODUCTION

The need to disseminate and transmit information is as old as humanity. The first paradigm shift happened with the appearance of printed books. The spread of the Internet among the population and the emergence of rapidly growing portals and social networks have made the second paradigm shift necessary. The emergence of ever-evolving smart devices is constantly changing people's needs [1]. It is now expected that a growing number of devices can be managed electronically. This is important in many areas of daily life, including education [2, 3].

The concept of Smart City includes the extensive serving of city dwellers, improving their quality of life, providing the most benefits with the smallest investment and making the environment more liveable in the long run [4], with the protection of the infrastructure and the individuals [5-7]. The development of the infocommunication infrastructure is essential for the implementation of the smart city concept. One of the purposes of the infocommunication system is the transmission of information. When forwarding information, not only the needed information is transferred, but it is also accompanied by additional information. This additional information is provided without intention [8]. In public communication, the final destination of the transfer is not a specific person or object. This way, anyone can obtain additional information. In the processing of information, additional information is often more important than intentionally transmitted information. The information displayed in this way is suitable for influencing, facilitating decision-making [9] and obtaining further information. Since such additional information comes from a completely open source, this kind of intelligence is called Open Source Intelligence (OSINT), which is one part of the social engineering methodology system [10].

Additional information will be defined in this study. In addition, an internet game will be presented to illustrate additional information. The game's summary is an example of how examining transmitted information from other angles can influence information acquisition. This gives an insight into the role of additional information in obtaining information.

ADDITIONAL INFORMATION

In communication, increasing transmission reliability emphasizes the importance of redundancy. In practical terms, therefore, the amount of data transmitted during communication is always greater than the amount required [8]. The expression of human thoughts and feelings is not exact, therefore, other supplementary clarifying information may appear during the communication containing them [10]. This means that the transmitted information may contain information other than what was intended by the initiator. The extra information that appears in this way has additional value in obtaining information, so it may serve as a basis for further research. There is no particular obstacle to obtaining this information through public communication and the intentional sharing of information. Moreover, this form of obtaining information does not violate the law, as the initiator deliberately shares the information [11-13].

Additional information can be defined as the information that appears alongside the content of the information that is intentionally conveyed, and there is an assay aspect system in which it represents added value.

The research aspects can also be grouped according to the abstract categories of information modelling: storage, processing and transmission [14, 15]. Another possible grouping is based on information architecture layers. Layers of the architecture include the energy layer, the layer of physical devices, the level of logical modeling and human behavior [8].

APPLICATION STAGES

Social engineering is a methodology that involves obtaining information, processing information in a targeted way [16], influencing decision-making [9, 10], and forcing organizational change.[17] One method of obtaining information in the methodology is open source intelligence [10]. This technique is one of the most convenient ways to obtain information.

There are many aspects to consider when processing information. For example, there may be additional information, other than those mentioned above, for a particular post. It can reveal the background of the human relationship, the temporal and spatial parameters of the actions and events, the physical, material and mental state of the actors. At the same time, obtaining information has become easier with the advent of social platforms. Curious acquaintances, journalists, marketing analysts, product development supporters and analysts, recruiters and personal practitioners also use open source intelligence. OSINT is a tool in the employers' repository as it can provide information about lifestyle and habits in addition to the information in the CV. For this reason, it is advantageous for employers to use community portals, which can provide additional information about applicants during the selection process, thus facilitating the decision.

Participation in community portals can also allow intervention. One of the bases of social engineering attacks is open source information. The additional information displayed above the mediated content helps to prepare and carry out a targeted attack. Obtaining and processing additional information can also facilitate targeted marketing, simple deception and fraud [11].

EXAMPLE OF FINDING LOCATION

Social portals and blogs are perfect tools for OSINT practitioners to obtain information. Published photos carry information about daily routines, habits, routes, locations, favorite foods and drinks, social networking and more. To illustrate this, an internet game was created by the authors of the study. During the game, players were required to determine the location of the photos from a series of photos. The photos were taken as dolls' selfies to avoid privacy issues.

The game was published as follows:

- the game was published anonymously using a nickname,
- the photos were publicated in a publicly available, viewable and accessible way,
- the photos did not contain metadata about the parameters of the creation,
- several photos were published during each game event,
- a given doll was used in multiple locations
- it was not announced where the doll was going to go or what the event was.

The photo montage in Figure 1 gives an example of the pictures taken during the game. The following statements were made:

- players responded to the game within 20 minutes,
- the region of the site was guessed within 30 minutes,
- the correct deciphering of the scene of the picture took more than 5 minutes,
- additional information appeared in the replies:
    - identification of the buildings on the site,
    - identification of the landmarks on the site,
    - the maker and the type of the doll used,
    - analysis of the originality of the doll's clothing.

Figure 1. Photo montage from the game.

After viewing the published images, players were also able to find out where the creator of the images was, and how often and in what orientation the creator travelled. Some more information included that the creator of the picture had at least three types of toy dolls in his environment. Collectors can easily determine the dolls' manufacturer and the types of dolls in the photos. Based on the above findings, it can be concluded that the images conveyed a great deal of information beyond the information needed to solve the game.

CONCLUSIONS

Urban development has brought about the need for sustainable and livable cities, which requires renewable infrastructure in the long term. Among others, this demand has led to the emergence of the smart city concept. The appropriate infrastructure is essential to realize this concept [1-4]. Like in other systems, the infocommunication infrastructure remains one of the most important infrastructures of smart cities.

One of the main purposes of the infocommunication system is the transmission of information [8]. When the information is transmitted, it is not only the required information

that is transmitted but some additional information is also disclosed with it. This additional information may be suitable to convey more meaning in a different aspect. For this reason, additional information is a basic source of obtaining information. One of the simplest forms of obtaining information is through public communication, the intentional sharing of information and broadcasting. Moreover, this is not against the law because the information is intentionally provided by the source [11-13]. This form of intelligence is OSINT.

The main driving force behind the need to obtain information is to influence decisions and enforce change. The process include information gathering, targeted processing and intervention. This process is completed by the methodology of social engineering [9, 10]. The game in this study is an example of how OSINT can be applied to obtain information through social media. During the game and at the end of the game, it was found that additional information can be obtained without major obstacles.

REFERENCES

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

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

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

[4] Tokody, D.; Schuszter, G. and Papp, J.: *Study of How to Implement an Intelligent Railway System in Hungary.*
In: Szakál, A., ed.: *IEEE 13th International Symposium on Intelligent Systems and Informatics: Proceedings*. IEEE, New York, 2015,
http://dx.doi.org/10.1109/SISY.2015.7325379,

[5] Kiss Leizer, G.K. and Berek, L.: *The Safety Technology Questions of Wastes Arising in the Course of Catastrophes in the Continental Traffic.*
In: Bitay, E., ed.: *Proceedings of the XXI-th International Scientific Conference of Young Engineers 2016*. Transylvanian Museum-Society, Cluj Napoca, pp.217-220, 2016,
http://hdl.handle.net/10598/29162, accessed 1st February 2019,

[6] Marrone, S.; Rodriguez, R.J.; Nardone, R.; Flammini, F. and Vittorini, V.: *On synergies of cyber and physical security modelling in vulnerability assessment of railway systems.*
Computers & Electrical Engineering **47**, 275-285, 2015,
http://dx.doi.org/10.1016/j.compeleceng.2015.07.011,

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

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

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

[10] Bansla, N.; Kunwar, S. and Gupta, K.: *Social Engineering: A Technique for Managing Human Behavior.*
Journal of Information Technology and Sciences **5**(1), 18-22, 2019,
http://dx.doi.org/10.5281/zenodo.2580822,

[11] 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,
[12] Pető, R.: *Security of Smart City.*
Interdisciplinary Description of Complex Systems **17**(1), 13-19, 2019,
http://dx.doi.org/10.7906/indecs.17.1.3,
[13] Kovács, Z.: *Cloud Security in Terms of the Law Enforcement Agencies.*
Hadmérnök **7**(1), 144-156, 2012,
[14] Kasac, J.; Stefancic, H. and Stepanic, J.: *Comparison of social and physical free energies on a toy model.*
Physical Review E **70**(1), 16117-16124, 2004,
http://dx.doi.org/10.1103/PhysRevE.70.016117,
[15] Albini, A. and Rajnai, Z.: *Modeling general energy balance of systems.*
Procedia Manufacturing **32**, 374-379, 2019,
http://dx.doi.org/10.1016/j.promfg.2019.02.228,
[16] 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,
[17] Pokorádi, L. andVányi, G.: *Sensitivity Investigation of Failure Mode and Effect Analysis.*
In: Jármai, K. and Bolló, B., eds.: *Vehicle and Automotive Engineering 2. Proceedings of the 2nd VAE2018.* Springer International Publishing, Heidelberg, pp.497-502, 2018,
http://dx.doi.org/10.1007/978-3-319-75677-6_43.

Interdisciplinary Description of Complex Systems 17(3-A), 444-457, 2019

MONITORING OPTICAL DATA CONNECTION BETWEEN PROTECTED ROOMS IN SMART CITIES

Gábor Bréda*

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

DOI: 10.7906/indecs.17.3.3
Regular article

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

ABSTRACT

The infrastructures of Smart Cities presuppose the existence of a basic IT data transmission network. This is also true for point-to-point connections between protected spaces in potentially different locations. The establishment of a stable IT connection is an essential element in the development of information infrastructures. Transmission bandwidth is a basic parameter to show the functionality and usability an IT system. As a result of advances in fibre-optic data technology, fibre-optic data connectivity solutions have now become standard tools, and due to their features, other technologies used for long distance connections have been almost completely eliminated by this technology. Continuous operation of fibre-optic connectivity has become vital to the operation of Smart City devices, as well as to the continued stable operation of critical infrastructures and protected spaces. Thus, the failure of an optical fibre requires immediate troubleshooting and corrective action from the operator. The scope of this research includes the basic methods of fault detection with regard to optical fibres, from simple methods to testing with the Optical Time Domain Reflectometer as a basic and important measurement method in the operation of optical data communication networks.

KEY WORDS

optical fibre, optical fibre monitoring system, protected room, optical time-domain reflectometer

CLASSIFICATION

JEL: L63, L94, L96
PACS: 84.40.Ua, 84.40.

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

INTRODUCTION

Regarding the info-communication transmission channels of Smart Cities of the 21st century, the most important trunking solution has now become fibre. This technology is a great tool not only for a leased line channel, due to its transmission bandwidth and ease of deployment, but it also allows the monitoring of continuous operation. Because of this feature, it is also suitable for realising point-to-point secure communication as a reliable physical channel for data transmission between protected rooms. By operating a thread monitoring system, it is possible to accurately determine the fault location in the event of a longitudinal parameter change or error. In addition to the implementation of telecommunication systems, the fibre-optic plant is also capable of ensuring protected communications depending on the signal encryption, as well as serving as a communication link for automated field systems having their own standards. This technology can be well utilised as the physical layer of the communication channel for information security-protected rooms, because by using cryptographic tools and running a continuous thread monitoring system, the point-to-point communication line can also be controlled for its physical parameters. Thread monitoring guarantees immediate detection and fault location of transmission channel malfunctions for long-distance connections of industrial automation. Another advantage of optical fibres is their insensitivity-free operation and ease of installation. A disadvantage is that only special target devices can implement continuity bonds. The purpose of this research is to systematise the theoretical solutions needed for detecting serial errors in optical fibres, and to review the basic application of a fibre monitoring tool.

Thesis 1: Today's primary trunked data transmission channel is the optical fibre.

Thesis 2: By implementing optical fibre monitoring, a safer and faster fault location detection can be achieved in case of serial errors.

Thesis 3: Fibre-optic communication is the safest way to secure point-to-point communication between protected rooms.

OPTICAL FIBRE CONNECTION AND ATTENUATION MEASUREMENTS ON THE OPTICAL FIBRE

Optical fibres can be classified according to various parameters which are very important in the design, operation and fault diagnosis of a system. In an optical network, there is always a transmitter device which is connected to the light transmission medium by means of at least one connector; in this case, the optical fibre, and then again, through a connector to a receiving unit, which receives the light pulses emitted by the transmitter, Figure 1.

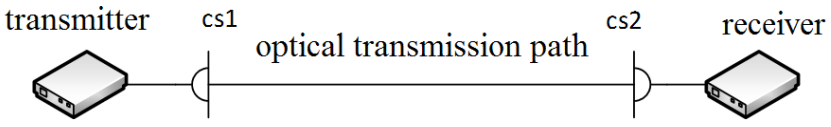

Figure 1. The most basic connection model.

This is the minimal set-up for a single fibre connection. However, a light connection is only established if the transmitter and receiver are capable of transmitting light signals with appropriate line attenuation. One of the most important parameters of a fibre is attenuation, since this value determines the maximum distance that can be travelled between the transmitter and the receiver without a repeater regenerator. Light suffers energy loss until it reaches the transmitter and the receiver. The attenuation rate is 10 times the 10-based

logarithm of the quotient of power transmitted at the transmitter side and the receiver-side output power of the end of the "l" optical transmission path, according to formula (1).

$$\alpha = 10 \cdot \log \frac{P_{be}}{P_{ki}}, \text{ [dB]}. \quad (1)$$

Since the fibre-optic network is a distributed parameter network, the equation can also be given per kilometre using formula (2) [1, 2, 11, 12].

$$\alpha = \frac{10}{l} \log \frac{P_{be}}{P_{ki}}, \left[\frac{dB}{km}\right]. \quad (2)$$

CUTBACK METHOD

For the cutback method, the first step is to make a measurement at the end of the optical fibre with a level meter in an assembly that is shown in Figure 2. The amount of light output from the level transmitter must be measured. Then, the optic fibre must be cut one meter from the transmitter, and have a connector attached to its end, as shown in Figure 3, and the transmitter signal power has to be measured again [13].

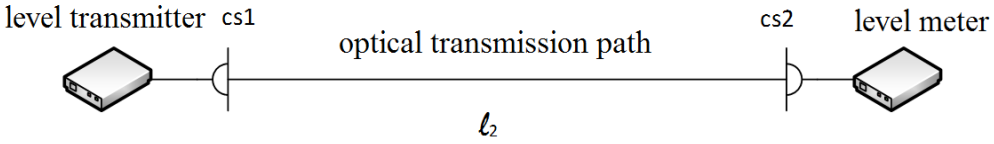

Figure 2. Measurement of fibre attenuation for the cutback method.

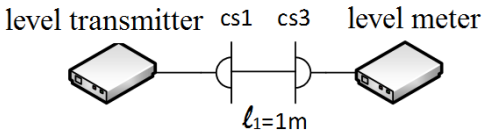

Figure 3. Measurement of fibre attenuation in case of a cut fibre.

From the results of the measurements, the attenuation per kilometre can be determined using formula (3).

$$\alpha = \frac{1}{l_2 - l_1} \cdot 10 \log \frac{P_{cs3}}{P_{cs2}}, \left[\frac{dB}{km}\right]. \quad (3)$$

INSERTION LOSS METHOD

The insertion method is theoretically very similar to the cutback method, but first the power of the leveller on a short thread is measured, then the level transmitter, as shown in Figure 4, and finally the level again at the fibre end. This is shown in Figure 5 [3-5, 14].

The fibre attenuation can be calculated using formula (4).

$$\alpha = \frac{1}{l - l_1} \cdot 10 \log \frac{P_{cs1}}{P_{cs2}}, \left[\frac{dB}{km}\right] \quad (4)$$

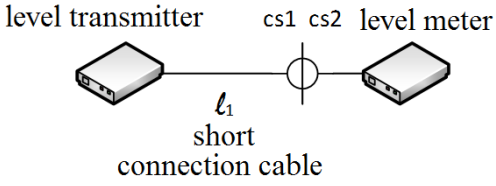

Figure 4. First measurement set-up for the Insertion Loss Method.

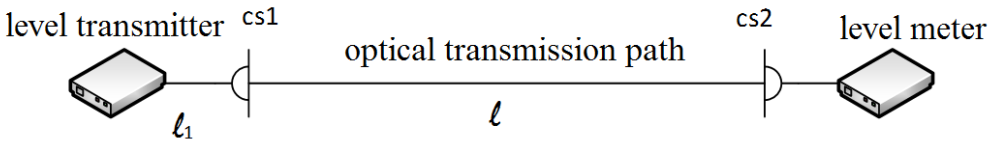

Figure 5. Second measurement set-up for the Insertion Loss Method.

Comparing the two measurements, the latter proves to be more appropriate, even during a plant measurement, since in this case the fibre to be measured does not have to be cut. When constructing optical cable networks, an attenuation test report must always be prepared for the future. In the event of an error, this is the first parameter to check. The simplicity of the measurement is a great advantage, while, the fact that it requires intervention at both ends of the fibre can be a disadvantage. In practice, it is advisable to connect the level transmitter and the level receiver to each other at the beginning of the measurement using a short measuring cable, and to set the reference levels relative to each other [6-10].

BACKSCATTER METHOD

Backscatter measurement has made significant advances in the determination of optical fibre parameters. This measurement principle is most significant, as modern optical cable management systems use this method to determine parameters and errors.

The method is based on Rayleigh scattering. A scattering occurs at the error location with virtually every change in the fibre parameters, which spreads power backward through the fibre. Scattering can be detected with a proper metering system. The attenuation or attenuations can be rendered visual over the entire length of the fibre over time.

The instruments suitable for this measurement technique are called Optical Time Domain Reflectometers (OTDRs). The measurement can be used mainly for the following purposes:

- determination of defective locations and their distances on optic fibres,
- measuring the attenuation of the connections,
- to measure the specific attenuation of optical fibres

By monitoring the backscatter, all significant features required for installation and operation can be determined. Furthermore, compared to the previous two attenuation measurements, in this case, the measurement can be done from one side, providing significant advantages for quick measurement.

The principle of the measurement is as follows: A narrow light pulse is applied to the fibre input. The light pulse propagates through the fibre, while the light is reflected to the input from every continuity defect and the end of the fibre. At the fibre input, where the light pulse was applied, we now connect a light-sensitive photodiode. From the backscattering signals that the photodiode can detect, we can render a visual representation plotted against time, as we know the speed of light propagating through the fibre [15, 16, 30].

A general block diagram of an OTDR instrument is shown in Figure 6.

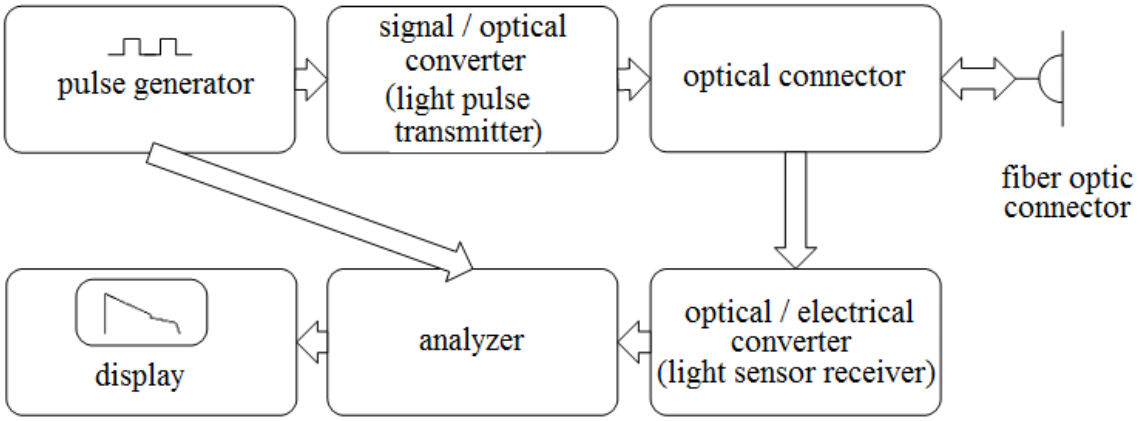

Figure 6. Block diagram of the internal structure of the OTDR.

If the fibre is constant throughout its length, the curve shows a steadily decreasing pattern. Jump peaks appear at the end and beginning of the fibre, as the refractive index of the fibre changes abruptly at these locations. In the inhomogeneous connection and bonding locations, where the kilometre-specific attenuation is different from the average, steps are forming on the curve. These are called reflective points. An example of a practical measurement by the OTDR instrument during the research is shown in Figure 7.

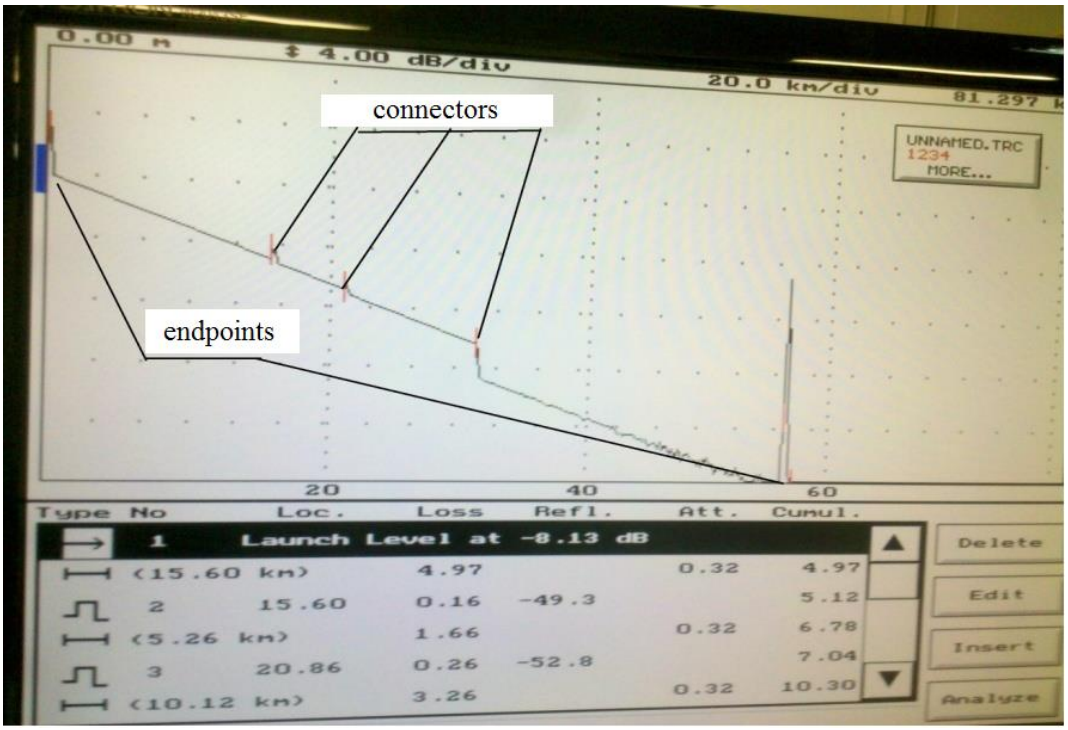

Figure 7. Screenshot of an OTDR measurement.

The length of the fibre can be determined from the start-end-start run time of the light pulses in the fibre. By measuring the time between peaks, the length of the fibre between the peaks can be calculated. The distance to propagation velocity can be calculated using the time differences and the refractive index using the following formula (5).

$$l = \Delta t \frac{c}{n}, \tag{5}$$

where *l* is the fibre length, c = 300 000 km/s; *n* is the refractive index and Δ*t* refractive index between peaks. The length attenuation can be read from the back-scattered length-performance diagram. This image is shown in Figure 7.

Figure 8 shows the basic fibre length attenuation measurement, which can also be calculated using formula (6), where l_1 and l_2 are the lengths of the measuring and the measured fibres, and Pl_1 and $P1_2$ are the power levels of the light pulses generated and received [17, 18].

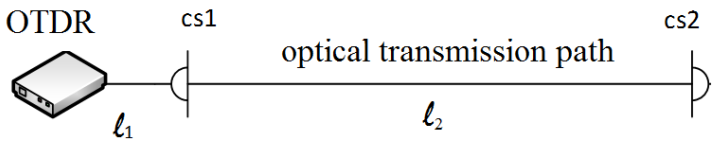

Figure 8. OTDR measurement.

$$\alpha = \frac{1}{2(l_2 - l_1)} \cdot 10\log\frac{P_{l_1}}{P_{l_2}}. \quad (6)$$

OTDR MONITORING OF OPTICAL TIME-DOMAIN REFLECTOMETER

In the course of the research, considering the state-of-the-art OTDR measurement technology, it became evident that there is a solution which allows the in-service monitoring of optical fibres. Such solutions include:

- Dark fibre monitoring when using WDM technology,
- Out-of-band monitoring,
- In-band monitoring,
- Broadband monitor port measurement

With the advancement of optical telecommunication devices, light sources with very narrow wavelengths were developed. These are typically capable of radiating the same wavelength with high stability to achieve a small chromatic dispersion. Later, it became possible to create multiple data transmission channels on an optical fibre by applying appropriate wavelength filters, thus significantly increasing the bandwidth. This is called WDM (Wavelength Division Multiplex) technology. Within this technology, the CWDM (Coarse Wavelength Division Multiplex) and DWDM (Dense Wavelength Division Multiplex) solutions are, in principle, the same, but differ in their wavelengths used for telecommunications. With CWDM, the channels are farther apart than with DWDM. The filters used to separate the wavelengths of the technology are called WDM filters. Figure 9 below illustrates three wavelengths for transmitting multiple wavelengths over a single optical fibre [27, 30].

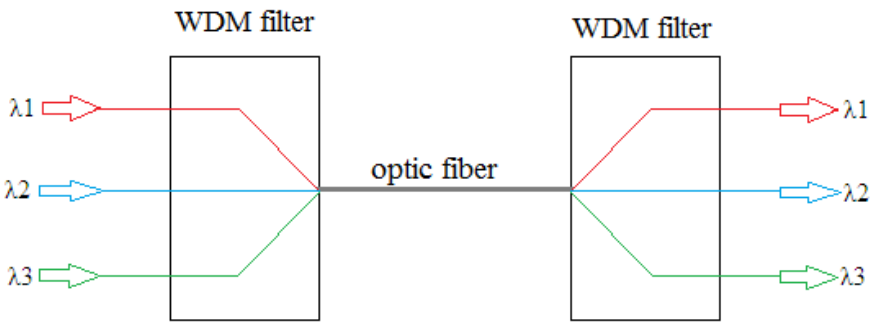

Figure 9. Tri-band WDM filter.

DARK FIBRE MONITORING

In the case of dark fibre monitoring, a backup fibre of a fibre-optic cable that is not used in telecommunication, or an unused fibre is measured with an OTDR instrument. This measurement provides accurate information on the continuity of the cable and changes in the assumed ageing and attenuation processes. There is no need for expensive filtering and coupling units, but one disadvantage is that it does not give a true picture of the state of the optical fibre that is involved in data transmission, which may be relevant. Of course, this is not a bad solution, since the parameters of the running fibre in a cable are the same and the monitoring of a single fibre within a cable provides about 98% security during business continuity checks. In a single cable, monitoring two strands means 99% security and monitoring three strands means 99,8% security. The implementation should consider the cost of the effort and the desired security.

The typical wavelength of the technology is the same as the standard wavelengths of 1310 nm and 1550 nm used in telecommunication. By using 1550 nm, the greatest possible measuring distance is achieved, because at this wavelength the attenuation of the optical fibres is the smallest. It can be implemented with an existing cable network, provided that it has an unused optic fibre. A simple schematic of the technology is shown in Figure 10.

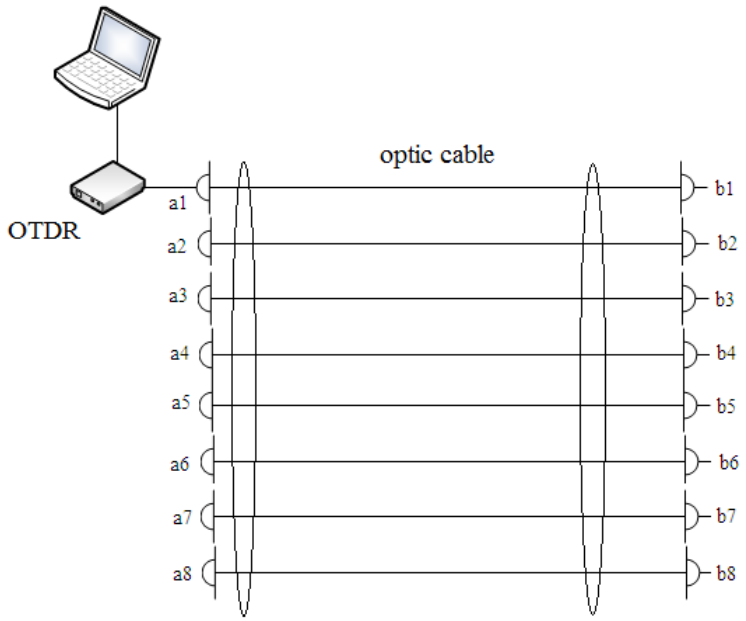

Figure 10. Simplified model of the dark fibre monitoring.

OUT-OF-BAND MONITORING

Out-of-band measurement is based on the principle of transmitting measurement signals to the 1650 nm band in the optical conductor fibre, over the last CDWM 1611nm wavelength channel, and displaying the reflected value on the OTDR display (Figure 11). Wavelength is more sensitive to attenuation originating from fractures and bends. The implementation of this technique requires filter units (WDM), so it is more expensive than the previous solution. A drawback of this technique is that if there are multiple branches in an optical fibre, the exact scattering and the backscattering resulting from the connection of the following elements cannot be well distinguished. It is advisable to implement it before installing the cable network. This method can provide 100% monitoring over the optical fibre involved in telecommunications [26].

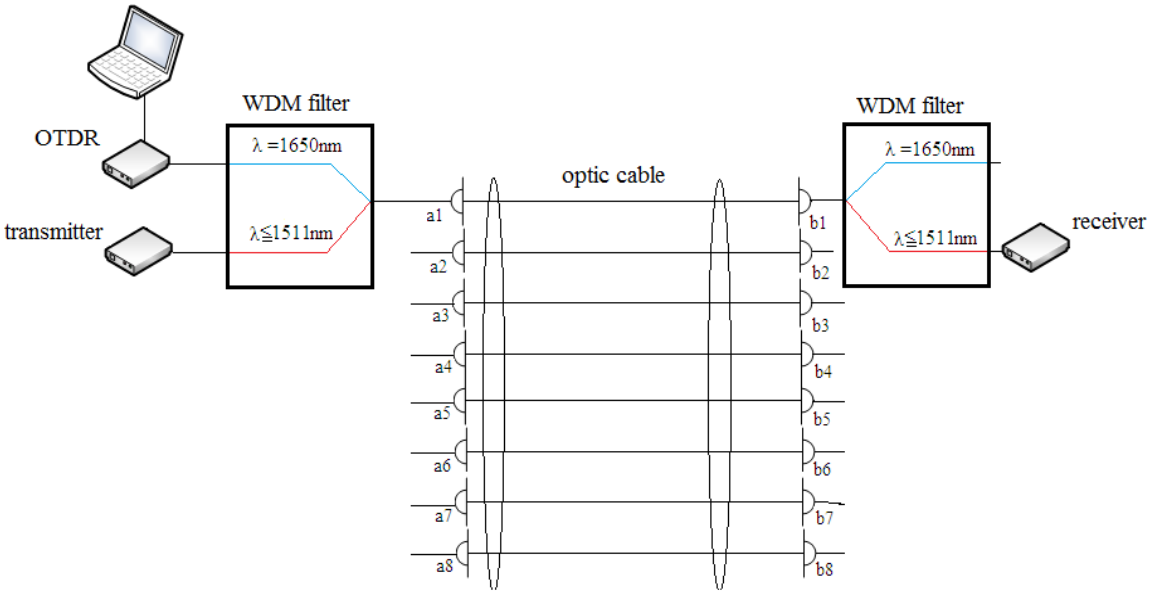

Figure 11. Simplified model of the out-of-band OTDR monitoring.

IN-BAND MONITORING

The implementation of this method is similar to the out-of-band method, but this technique uses one or more of the data transmission wavelengths, depending on the implementation. Figure 12 is a conceptual diagram of the monitorability of a branched optical fibre. The figure shows that there are 5 different λ wavelengths added to the cable using a "WDM filter 1". The different wavelengths are marked with different colours for the sake of illustration: λ1 pink, λ2 blue, λ3 red, λ4 green, λ5 orange. λ1 and λ2 are the wavelengths of the OTDR, while λ3, λ4, λ5 are the wavelengths of the data transmission. If there is a branch in the light guide, which is referred to as "WDM filter 2" in this figure, the branches can be separated by the proper selection of wavelengths and the application of the appropriate WDM filter. As shown in the figure, following the upper branch of the "WDM filter 2", λ1 and λ4 (of which λ1 marks the OTDR monitor and λ4 is the data carrier) are passing through. Following the lower branch, λ2, λ3, λ5 are passing through (λ2 is the OTDR monitor; λ3 and λ5 are the data carriers).

The filters called "WDM filter 3" and "WDM filter 4" separate the appropriate wavelengths for the terminals so that the signals used for data transmission and monitoring do not interfere.

By switching between the λ1 and λ2 wavelengths of the OTDR instrument, the parameters of the given section can be examined. In case of the λ1 OTDR test signal, the line "WDM filter 1" – "WDM filter 2" – "WDM filter 3" can be monitored. In case of the λ2 OTDR test signal the monitoring of the line "WDM filter 1" – "WDM filter 2" – "WDM filter 4" can be ensured.

This example illustrates that multiple optical wavelength signals can be transmitted on an optical fibre. A disadvantage is that the wavelengths used for the measurement cannot be used for data transmission. However, branched optical fibre monitoring can be implemented by changing the OTDR output wavelengths. The measurement system can be installed even in networks with built-in WDM filters. The transmission wavelengths need to be taken into account, and a narrow bandwidth optical signal is required [26].

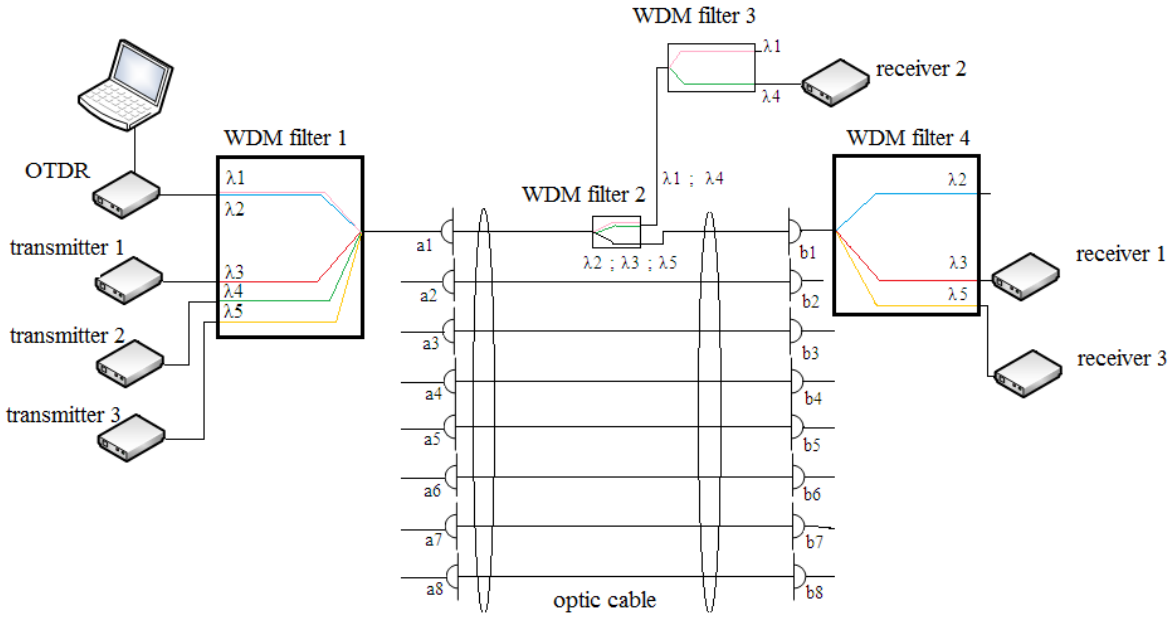

Figure 12. Simplified conceptual model of the in-band OTDR monitoring.

MEASUREMENT VIA BROADBAND BRANCH-LINE COUPLER

At the endpoints of optical networks, full-band and wide-band junctions are used to monitor port traffic (Fig 13). The input and reception of a measurement signal on this device allow the implementation of the OTDR measurement. The measurement signal entered here is also sent and received using a separator (WDM) filter, considering that the wavelength of the measurement signal does not coincide with the wavelength of the data transmission signal. From an implementation point of view, the input signal is fed to the receiving side of the data transmission to avoid interference.

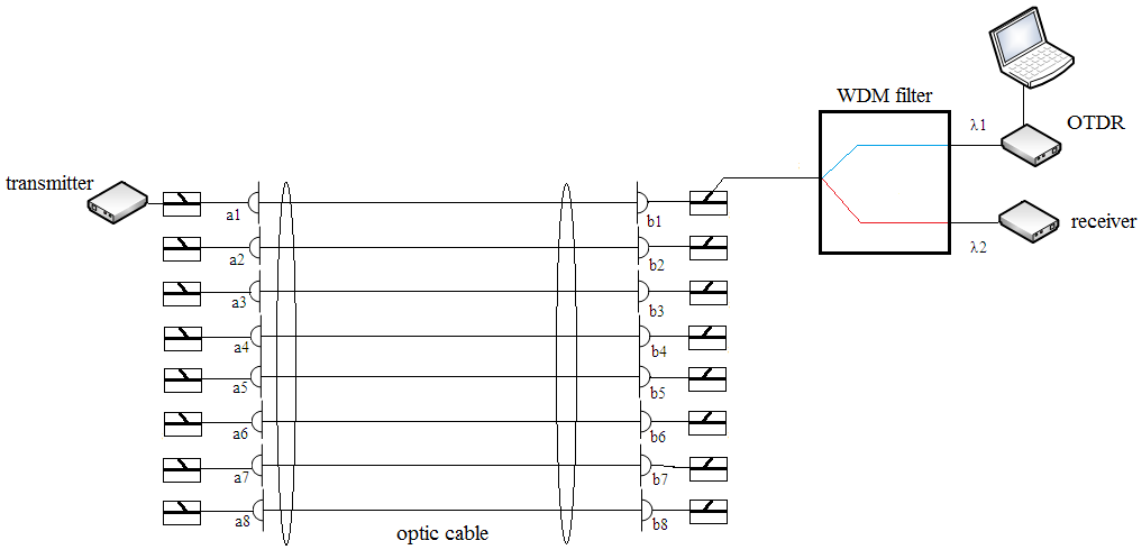

Figure 13. Conceptual model of an OTDR monitor installed into a branched network.

USING AN OPTICAL SWITCH TO EXTEND FIBRE MONITORING

In case of the above examples, the OTDR fibre monitoring was tested on single fibres. However, with full control, each fibre would require its own OTDR instrument. This costly solution can, however, be circumvented by the use of a fibre switching device, without which these advanced fibre management solutions could not be implemented.

The Optical Test Access Unit (OTAU), which operates on the principle of a multiplexer, is an OTDR-controlled fibre switching device that couples the instrument providing the measurement signal to the fibre to be monitored. With the help of appropriate software control, the fibres are switched on, and the continuous measurement is ensured by repeated monitoring. Figure 14 illustrates the operation of the optical switch. The desired OTDR input signals can be set for the channels and a reference value can be recorded during installation, with regards to the measured values and diagrams. If the unit detects an error relative to the reference, it will immediately generate an alarm. In case of this technique, the way fibres queue up to be examined depends on the frequency of switching. The shortest amount of time while a problem could be detected is equal to the amount of time the same fibre is tested again [29].

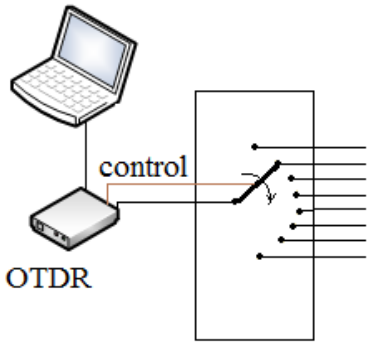

Figure 14. Conceptual model of an optical switch.

Further improvements point to the increase of the speed of error detection. Accordingly, continuous power measurement is performed on the receiving side of the controlled optical fibres. Power levels are taken as reference during installation. The power meter is connected to the OTDR controlling computer to form a complete monitoring unit. If the continuous power meter detects a slip from the reference, the OTDR is immediately directed to the fibre for testing. This eliminates the time gap that occurs in case of an unfavourable switching order [19-23].

FAULTS AND CHARACTERISTICS OF OPTICAL NETWORKS

There are various approaches to classifying the faults in optical networks. However, in our case, the most important type of error is increased line attenuation. The maximum power emitted by the transmitter does not reach the receiver unit at the proper level due to the increase in attenuation. Negative changes in attenuation are possible due to:

- change in fibre characteristics,
- degradation of connectors,
- changes in transmitter power and receiver sensitivity

CHANGE IN FIBRE CHARACTERISTICS

The attenuation of optical fibres may vary mainly due to the physical effects on them.

Material structural stresses are induced due to the twisting and shear forces on the cable. These stresses create inhomogeneous sections in the fibres, which result in local attenuation sites.

Another typical defect is the exposure of the cables – and thus the fibres – to high fibre tensile forces. This effect also leads to material structure issues. If a fibre-optic cable and its fibres are damaged by longitudinal contact, the entire section may become unusable [24].

Transverse rupture of the fibres may occur during construction, e.g. being cut through by a machine. Of course, this leads to a complete rupture, which can be repaired by fibre welding or section replacement.

Improper cable routing can also result in an increase in attenuation by breaking below the smallest bend radius. In this case, if the fibres do not suffer permanent damage, the attenuation resets to its original state once the error is eliminated. These errors are called macrobanding errors.

DEGRADATION OF CONNECTORS

Each optical system connects to network components using connectors. These connectors vary by cable types. Typically, faults in connectors can be traced back to mechanical faults and/or issues caused by dirt getting into the network. The fibre ends in the connectors can be flat, rounded (PC, UPC), or bevelled (APC), Figure 15.

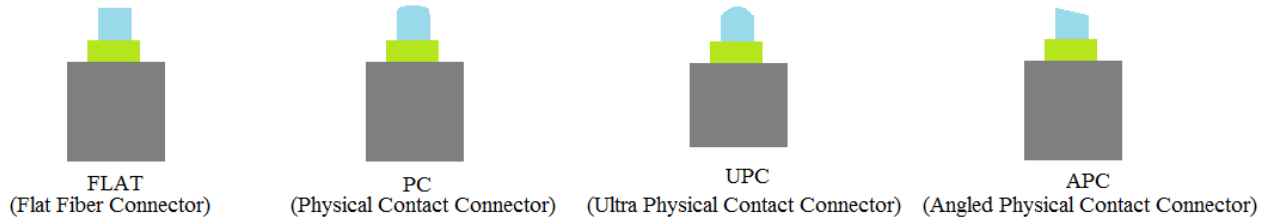

Figure 15. Connector types.

The alignment of the connectors greatly determines the attenuation value. If a centrality error or large air gap develops, the refractive index changes between the two photoconductor cores, and causes unwanted attenuation in the transmission path.

Furthermore, it must be ensured that the connection of the connectors is uncontaminated, as attenuation error occurs when contaminants go between the contact surfaces [30, 32, 33].

CHANGES IN TRANSMITTER PERFORMANCE AND RECEIVER SENSITIVITY

In this case, the error occurs on a device that is not dependent on the attenuation of the optical network in question. This type of error means damage to the terminal equipment, which can be solved by replacing or repairing the units [25, 28].

OTHER DEFECTS THAT CAN BE DETECTED BY THE OPTICAL FIBRE MONITORING SYSTEM

In addition to the errors listed above, optical fibre monitoring can detect slow or intermittent attenuation errors. This means that an alarm threshold is set as a reference value for the entire line segment taken during the installation of the monitoring system. When the controlled fibre attenuation reaches the set value of – 3 dB difference threshold, the control panel generates an alarm.

Continuous thread monitoring can also detect errors that are difficult to detect with other intermittent OTDR solutions. If the error does not occur for most of the time or the fibre

parameter does not deviate significantly from the reference value, then there are only brief moments when the attenuation increases somewhere in the fibre.

Such an error may be a mechanically unstable connector which, when periodically moved, results in a significant attenuation or intermittent breakage of the optical fibre when it is, for example, pinched by or pushed up against some parts of the rack cabinet.

Such continuous fibre monitoring equipment is also an essential means of protecting optical fibres from an information security point of view. Attempt to intercept optical fibres may be accompanied by an attenuation error that requires branching or bending. The resulting attenuation may also be detectable. If the alert threshold for monitoring is sufficiently sensitive, then the appearance of a small amount of attenuation can be immediately and automatically detected [31].

SUMMARY

The subject of the present article is one of the fastest-growing, but also quite challenging technical solutions for data transfer in smart cities. The fibre-optic used in light communication has been overcoming its limitations and disadvantages since its first appearance. Because of its advantages, this technology is an essential physical layer of info-communication in rooms protected from the point of information security. The study presented in this paper summarizes the principles related to the measurement of optical fibre attenuation. It describes the measurement of the backscatter attenuation and the measurement methods that can be implemented with OTDR. It then examines the potentials and characteristics of optical networks. The research and its summary have a great importance, as the technology and the monitoring system in question are slowly taking over the role of the physical layer of longer-range info-communication devices, making a significant leap in the quality parameters of telecommunications. Comparing the theses of the research with the above findings, the correctness of the theses can be logically deduced.

REFERENCES

[1] Cebe, L.: *Fénytávközlés*.
Kandó Kálmán Műszaki Főiskola, Budapest, 1990,
[2] Smigura, L.: *Távközlő kábelek és vezetékek*.
Magyar Posta Könyvkiadó, Budapest, 1989,
[3] Jutasi, I.; Vámos, P.; Márkus, E.; Tarnay, K. and Nádorfi, Gy.*: Fényvezető távközlési rendszer tervezése (CCITT)*.
Távközlési Könyvkiadó, Budapest, 1991,
[4] Gyárfás, A.: *Optikai elemek mérése EDUCOPTIC mérőberendezéssel.*
Budapesti Műszaki Főiskola Kandó Kálmán Villamosmérnöki Főiskolai Kar, Budapest, 174/1997, 2006,
[5] Gárfás, A.:*Optikai szálak mérése OTDR-rel.*
Kandó Kálmán Műszaki Főiskola, Budapest, 176/197, 1997,
[6] Lajtha, Gy. and Szép, I.: *Fénytávközlő rendszerek és elemeik*.
Akadémiai Kiadó, Budapest, 1987,
[7] Ákos, Gy.; Jani, P. and Varró, S., eds.*:Lézerek tudományos és gyakorlati alkalmazása*.
Prosperitas Kft., Budapest, 1993,
[8] Antók, P. I.: *Fényvezető Kábelhálózat Építése.*
Vonalas füzet, Mackensen Kft., Budapest, 2009,
[9] Elek, A.: *Nyomvonalas távközlési hálózatépítési technológiák kézikönyve*.
Magyar Elektronikai és Infokommunikációs Szövetség, Budapest,2006,
[10] Antók, P.I.: *Fényvezető Hálózatok Gyakorlat 2. Passzív és aktív elemek a gyakorlatban*.
Budakalász, 2011,

[11] Antók, P.I.: *Fényvezető Hálózatok II. Fényvezető hálózat alapismeret,*
Antók Mérnöki Iroda Kft., Budapest, 2011,
[12] Antók, P.I.: *Fényvezető Hálózatok VI., Fényvezető hálózatok létesítése II.*
Antók Mérnöki Iroda Kft., Budapest, 2011,
[13] Antók, P.I.: *Fényvezető Hálózatok VIII., Fényvezető hálózatok tervezése II.*
Antók Mérnöki Iroda Kft., Budapest, 2011,
[14] Antók, P.I.: *Fényvezető Hálózatok IX. Szélessávú Optikai Hálózat Tervezése, Méretezés.*
Antók Mérnöki Iroda Kft., Budapest, 2011,
[15] Choquet, L.: *Reference Guide to Fiber Optic Testing, Glossary*.
JDSU Corporation, 2008,
[16] Laferriére, J.; Lietaert, G.; Taws, R. and Wolszczak, S.: *Reference Guide to Fiber Optic Testing.* Vol. 1.
JDSU Corporation, 2007,
[17] Collings, B.; Heismann, F. and Lietaert, G.: *Reference Guide to Fiber Optic Testing.* Vol. 2.
JDSU Corporation, 2010,
[18] NTest Inc.: *User Guide: NTest FiberWatch RFTS System-0904.*
[19] Fiber Optics For Sale Co.: *Fiber Optic Cable Tutorial.*
http://www.fiberoptics4sale.com/Merchant2/fiber-optic-cable.php, accessed September 2018,
[20] Mediadot Kft.: *Optkai kábelek, Sommerkábel.*
http://www.sommerkabel.hu/optikai-kabelek-leiras.html, accessed October 2018,
[21] NTest Inc.: *Dark Fiber Monitoring.*
http://www.ntestinc.com/darkfiber.html, accessed September 2018,
[22] EXFO Inc.: *Live Fiber Monitoring in CWDM Networks, Olivier Plomteux, Senior Product Line Manager, Optical Business Unit.*
http://www.ccontrols.ch/cms/upload/downloads/Telecom/1206EN_FiberGuardianAplicationNoteLiveFiberMonitoringCWDM.pdf, accessed September 2018,
[23] Kozischek, D. and Bolick, M.: *Planning Link-Loss Budgets Using Statistics, Broadband Propertier*.
http://www.broadbandproperties.com/2007issues/jun07issues/corning_june.pdf, accessed July 2018,
[24] *Optical Components: Light Amplifiers.*
http://ftp.utcluj.ro/pub/users/cemil/dwdm/dwdm_Intro/8_5311715.pdf, accessed September 2018,
[25] Atcom Services, Inc.: *Fiber Optic Cable*.
http://www.lanshack.com/fiber-optic-tutorial-cable.aspx, accessed August 2018,
[26] 3M: *3M™ Planar Light Circuit (PLC) Optical Splitters*.
http://multimedia.3m.com/mws/mediawebserver?66666UuZjcFSLXTtmxfcOXM6EVuQEcuZgVs6EVs6E666666--, accessed October 2018,
[27] The Telecommunications Industry Association: *Standard: TIA/EIA Standard; Commercial Building Telecommunications Cabling Standard; April 12. 2001*.
http://www.nag.ru/goodies/tia/TIA-EIA-568-B.1.pdf, accessed May 2018,
[28] Triple Play: *Fibre Formulas made simple*.
http://www.tripleplay.co.za/uploads/Optical%20Fibre%20Formulas.pdf, accessed October 2018,
[29] NTest Inc.: *Active Fiber Monitoring*.
http://www.ntestinc.com/activefiber.html, accessed October 2018,
[30] Pieter, N.J.M.J., et al.: *Small Bandwidth OTDR.*
http://www.nikhef.nl/~jelle/antareswebdocuments/Sb_otdr/SB-OTDR.pdf, accessed May 2018,
[31] EXFO Inc.: *Live Fiber Monitoring in CWDM Networks—Part 2.*
http://www.exfo.com/corporate/blog/2010/live-fiber-monitoring-cwdm-networks-part-2, accessed September 2018,
[32] Varghese, S.; Priyamvada, M.; Mathew, M.; Swarish, N. and Suresh, N.: *A novel real--time Remote Fiber Monitoring System NeST Research & Development Centre*.
http://een.iust.ac.ir/profs/Sadr/Papers/netp9.pdf, accessed October 2018,

[33] Hell, P.M.; Varga, P.J. and Illési, Zs.: *Mobile Phones Thermo-Ergonomic Analysis.* In: 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics. IEEE, Subotica, 2018.

Interdisciplinary Description of Complex Systems 17(3-A), 458-467, 2019

DRONE SYSTEMS FOR FACTORY SECURITY AND SURVEILLANCE

Péter Miksa Hell and Péter János Varga*

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

DOI: 10.7906/indecs.17.3.4
Regular article

Received: 7 February 2019
Accepted: 31 August 2019.

ABSTRACT

Nowadays, when preparations and implementations are under way for smart cities, the use of drone systems in the safety of factories has come to the fore. Factories and industrial areas are complex systems. Physical control is essential for their optimal and safe operation. Most of the inspections can be performed with the use of human resources. However, efforts should be made to minimize the human factor in order to make the system as automated and optimized as possible. Pre-programmed routine tasks can be performed by drones, both indoors and outdoors. Dedicated drones are already in use around industrial facilities, primarily for facility protection. However, in enclosed halls, it is not easy to provide these tools with routine tasks, because indoor labor – material handling, reconnaissance, and accident-free transport – requires orientation. Besides the production lines and inside warehouse buildings, drones are already commonly used to perform smaller tasks, but the goal is to ensure the right ratio in the human-machine relationship. In their technical implementation, modern drones are assisted by various sensor systems (lidar, ultrasound, camera) that they are equipped with. This article presents the application of task-specific drones in industrial areas, both indoors and outdoors.

KEY WORDS

drone, smart city, factory, security, surveillance, indoor environment

CLASSIFICATION

JEL: L63, L92

*Corresponding authors, η: varga.peter@kvk.uni-obuda.hu; -;
Óbuda University, Tavaszmező u. 15-17., H – 1084 Budapest

INTRODUCTION

We have seen many examples of outdoor use of drones in recent years. From hobby flight systems to special drone systems, the field of application is very wide. Nowadays, the issue of outdoors orienteering has already been resolved and is supported by GPS, but in the framework of the Industry 4.0 concept, there has been an increased demand for indoor navigation of drones. When it comes to indoor use, you have to face the limitations that are not encountered during outdoor use. One of the biggest problems when trying to ensure safe indoors flight is to determine the appropriate position and reference points [1, 2].

INDUSTRY 4.0 AND DRONES

The Fourth Industrial Revolution directs us towards intelligent manufacturing, that uses information technology to change the way products are produced and reduce costs, and by doing so, it is focusing on efficiency [3, 4]. By accessing real-time data, companies can respond more quickly to customer interactions and product use interactions. Industry 4.0 is primarily about new technology and new innovative business models. During production, a single drone can be used in complex systems as a mobile sensor that transfers data from physical production processes to production control. Manufacturing companies have already used autonomous robots in the production and handling of products. Autonomous entities become more and more widespread [5-7]. A specially equipped drone works like a flying robot. Such a device can be integrated into assembly and manufacturing workflows to enable companies to operate more easily, efficiently and safely. Integrating drone technology into industrial manufacturing and control processes is becoming increasingly important. Figure 1 shows the rate of use of drones in the current market [8, 9].

Drones can become an integral part of industrial controls, as they can perform a task without human intervention for long periods of time in difficult to access or unsafe locations. Using high-definition cameras and Internet of Things (IoT) tools, drones can quickly identify key control points and provide information about the target being checked. Thanks to bidirectional

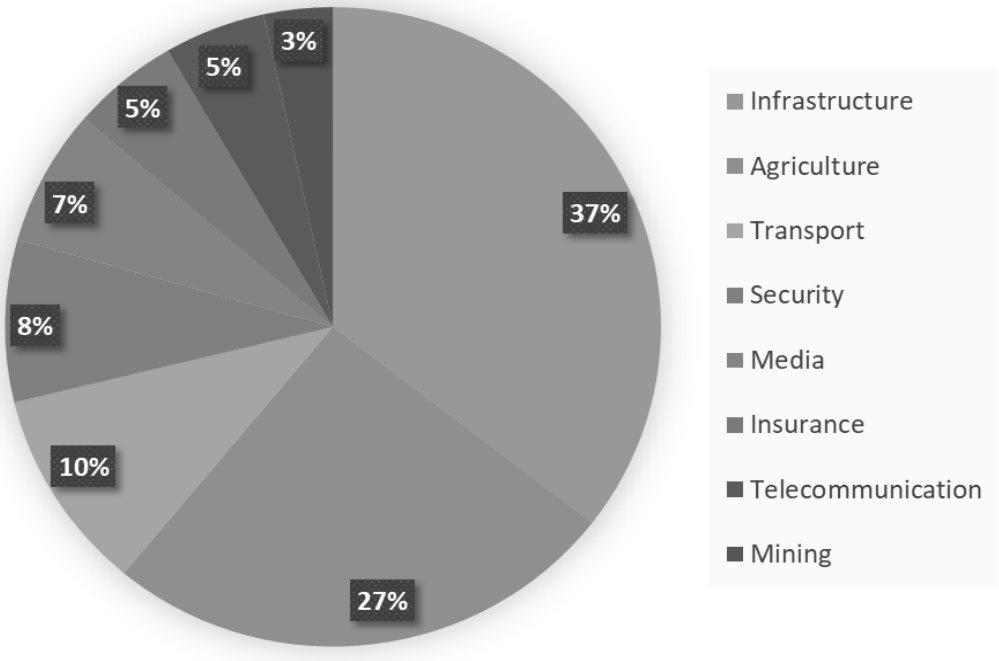

Figure 1. Drones in construction 2018 [10].

communication, the IoT platform provides an opportunity to analyze data immediately and identify problems. This autonomous drone, created with this knowledge and insight, is a preprogrammed aircraft that is capable of self-handling without operator intervention [11].

Hardware and software conditions required for fully safe collaboration of people and drones and the integration of drones in the production process:

- secure flight in an indoor, enclosed area with sensors, cameras, and intelligent object recognition and collision prevention algorithms,
- immediate situation recognition and real-time response to unexpected situations and obstacles ,
- the ability of drones to connect and communicate with other drones, machines, devices and people via IoT devices mounted on board,
- recognition and identification of the assigned markers,
- ability to make decisions independent of the pilot using artificial intelligence,
- automatic data upload and synchronization with a cloud-based database,
- flight time – battery capacity optimization,
- modularity. Drone configurations should be plug-and-play configurable to work as a module that can be added to existing processes.

OUTDOORS ORIENTATION

When it comes to outdoors, orientation is perfectly solved nowadays with Global Positioning System (GPS) and Global Navigation Satellite Systems (GNSS). Satellite positioning allows us to determine the right position via different kinds of GPS and Glonass. The accuracy is only a few centimeters. This can be further enhanced by a combination of Real Time Kinematic (RTK) systems. GPS is sufficient for outdoors orientation and positioning, but not for recognizing obstacles in the flight path. There is a simple reason behind this. When it comes to GPS and GNSS, the codes transmitted from satellites do not contain any land-based feature information. Also, the GPS receiver's map database does not include the exact location of the features. GPSes work reliably, but their operation depends on outside organizations. If for some reason these systems do not broadcast information or deliberately send incorrect information to the GPS receivers, then the whole system becomes inoperative. Figure 2 shows a flight route plan around a factory. The observation drone keeps track of the landmarks in a safe height and distance along the route only with the help of GPS. This can be combined with a sensor system placed on the drone.

GPS cannot help drones to perform tasks without collision in an industrial facility or within a building. Only various proximity sensors mounted on the drone are a solution for detecting and responding to various obstacles in the flight path. The real-time data from the sensors is processed by the flight controller, which then either corrects the flight path for accident avoidance or entirely stops the drone. In premium category drones, the default setting for the Security Proximity Sensor is to override the pre-written flight plan or the drone pilot command in case of a possible collision [12, 13]. These sensors operate on a variety of measurement principles, ranging from a simple ultrasonic Doppler-effect rangefinder to the intelligent object recognition algorithm of today's state-of-the-art 3D camera image analyzer [14-16].

On-board sensors for supporting drone stability and autonomy

Autonomous sensors ensure the stable flight and floating of the drones. These sensors are not connected to a global system such as GPS. The drone's flight controller processes and evaluates the data sent by the sensors then decides based on a pre-written or learned algorithm. The sensor data can only be sent for monitoring to the drone pilot or the drone control

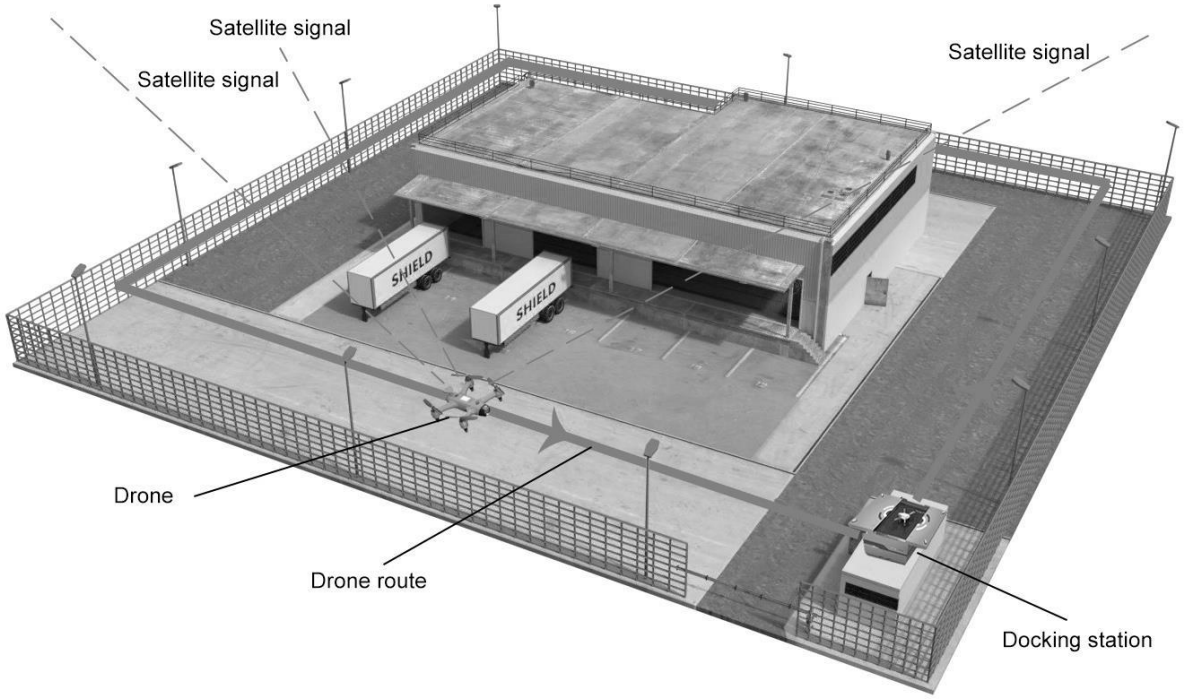

Figure 2. Drone performing a routine task using GPS.

control system. Even the simplest drone requires simultaneous processing and evaluation of multiple sensor signals for air retention and positioning [17].

Gyroscope

There are many gyroscopes that use different physical phenomena, such as rotation speed. To date, these devices have been completely replaced by the most common microelectromechanical systems (MEMS-systems) created by the combination of small microelectronics and mechanics. MEMS-type gyroscopes keep a small mass in constant vibration and regularly measure the deviation for the initial vibration plane. The differences are measured by the determination of the Coriolis force known in physics.

Accelerometer

The geometric size of the MEMS accelerometer sensors allows us to combine the sensor with other sensors for more accurate positioning. Their operation is very similar to the operation of a gyroscope. Inside the sensor, there are two comb structures that form a series of capacitors. When the sensor detects acceleration, the mass moves and causes a change in the capacitance of the capacitor.

Magnetometers

The principle of MEMS magnetometers is based on the Hall-effect. If a current flows in a conductor or a semiconductor and is placed in a magnetic field, the Lorentz force acts on the particles carrying the current, so there is a potential difference on both sides of the conductor. This potential difference can be measured.

Barometer

Most barometers used in drones are piezoelectric barometers (based on the MEMS system). A piezoelectric insert is located behind an opening in a cavity, completely blocked from its surroundings. In this cavity, an air mass value is recorded as a reference value. With the

change of height, the air pressure also changes, which deforms the piezo tile and results in a measurable electrical potential difference proportional to the air pressure.

Ultrasonic distance meter

The ultrasonic distance meter operates on the principle of the Doppler effect. The transmitter of the device transmits in the ultrasound range (40 kHz), which is reflected from the objects into the receiver. The electronics calculate the subject distance based on the timing of the reflected signals. In drones, these sensors are usually used as a ground-level altimeter or to avoid large obstacles such as walls or ceilings. This is one of the most important elements of indoor orientation. The advantage of the ultrasonic distance meter is that it is accurate even in poor visibility due to its operating principle. Its disadvantage is that its operation is only reliable for a few meters, and smaller, thinner objects such as electric wires are not noticed by it.

Optical flow

Continuous images recorded with the camera enable the speed of the drones to be measured. Their operation is very similar to that of a computer mouse. A low-resolution camera (below 1 MP) produces images at a very high refresh rate and produces a difference image using an algorithm. The two consecutive images and the change in time determine the horizontal speed of the aircraft. The accuracy, in this case, is determined by the processing algorithm, the quality of the images and the refresh time.

Stereoscopic cameras

With the advancement of technology, not only high-resolution cameras are available to be mounted on board, but also special recording cameras. They analyze images with artificial intelligence algorithms and directly help with navigation. Two-camera distance measurement is based on photogrammetric principles. By highlighting the common characteristic points of the two images, an algorithm can be used to determine the distance between the objects in the image. The quality of the finished dot net is the same as that of the cameras. This technological element is usually used to avoid obstacles, although it can also be used for 3D mapping of the environment.

LIDAR

LIDAR (Light Detection and Ranging) is an optical space mapping technology that lets you determine the distance of objects. Laser light consists of a pulse emitting transmitter and an optical sensor facing in the same direction that reads the reflected laser pulses. The measurement works on the principle of the Doppler effect. The narrow opening combined with a 360-degree rotating motion allows LIDAR to construct a complete panoramic image of its environment.

LEDDAR

The LEDDAR (Light-Emitting Diode Detection And Ranging) sensor is a further developed version of LiDAR technology, without the complex rotating mechanics. There is a great future ahead for this new generation device in Geographical Information System. Due to its size and price, it could be the most reliable sensor for drones. The angle of view depends on the optics. The sensor device can detect multiple objects simultaneously and determine their distance with millimeter accuracy. Depending on the angle of view, it detects objects up to 100 meters away. Obstructive objects nearby are illuminated by the built-in infrared, so the sensor can also be used in the dark.

Flight modes

Table 1 shows the general flight modes of advanced drones, outdoors and indoors [18].

Table 1. Flight modes for drones for outdoors and indoors. Light shaded – flight is not dangerous, dark shaded – flight is dangerous, flight mode is not optimized for the location.

Manual mode	Outdoors	Indoors
Full manual mode		
Manual mode with proximity sensor data		
Manual mode - except for No-fly Zone		
Automatic mode		
Automatic mode based on route plan, no proximity sensor		
Automatic mode based on sensor data		
Emergency flight mode		
Return on the shortest route with Ascension and Go Home function		
Return due to deviation from automatic travel direction		
Return due to a technical problem		

Positioning and navigation within buildings

GPS systems are well known in the determination of outdoor location. However, positioning inside buildings is a major challenge. The satellites usually do not reach the covered areas and the system would be unusable anyway due to interference. For these reasons, indoor positioning systems have received increasing attention over the past decades. The safe operation of indoor forklift trucks, such as servo robots and controlled trucks, is based on sophisticated technology. Due to the two-dimensional space of maneuver and the low speed of robots, the number of unexpected incidents causing accidents is negligible. However, this is not always the case for drones. In addition to the horizontal two-dimensional movement, these devices can move in a vertical direction, and are also faster, so, the security requirements for indoor drones are much higher [19, 20].

Indoors, task-specific drones use a particular, dedicated path to perform their task. Tasks may include taking pictures or videos of objects, material handling, workflow, and people. In order for the drone to safely perform its assigned task, the control system must continuously know the current position of the device with centimeter accuracy. An unexpected event may occur at any time on the assigned route, to which the drone must respond immediately. For indoor flight planning, we need to be aware of all the landmarks (such as walls, furniture, machinery, conveyor belt) that are present where the drone system is being implemented. The location of landmarks greatly influences flight operations (eg material handling, tracing). In order to avoid a collision between drones and landmarks, zones in which the airplane can move freely, and zones where the flight is prohibited must be selected during the training phase. If the path of the starting point and the point of arrival or route alternatives are unknown during task completion, route optimization cannot be performed in advance. In addition, if an unexpected obstacle also affects the direction, then the execution schedule of the planned tasks will also change [21].

For these reasons, indoor positioning systems have received increasing attention over the past decades. The position of an object placed in a three-dimensional space can basically be determined by two principles. Either the object determines its own position in space, or we determine the position of the object from the outside. The first version is ideal for drone systems because coordinate information must be processed directly on the drone. Figure 3 shows

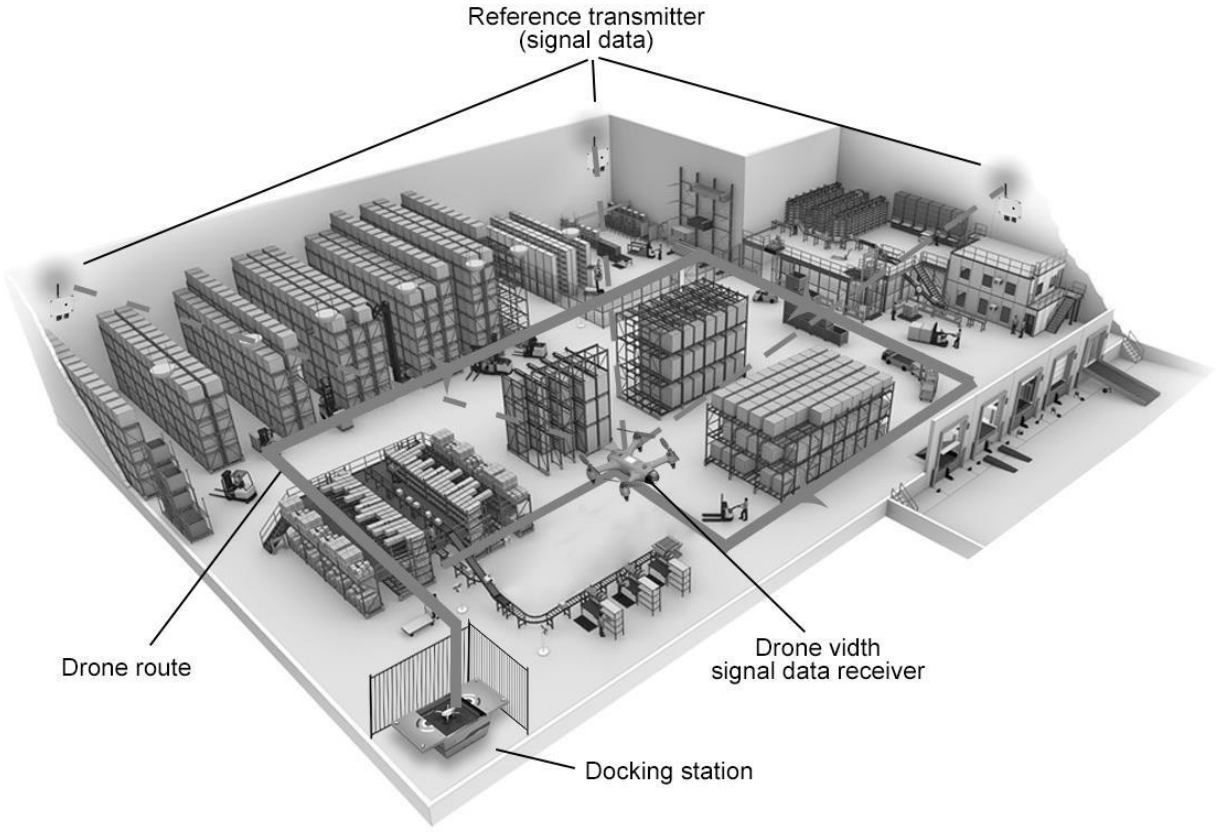

Figure 3. Drone performing a task based on a roadmap using indoor positioning [10].

the elements of an indoor location system. In a confined space, fixed transmitters emit a unique code sequence into the space that the drone sensor receives and the device calculates the exact position of the receiver unit (drone) based on an algorithm [22].

There are many different positioning systems based on infrared, ultrasound, RFID, ZigBee, and Bluetooth technology, each with its advantages and disadvantages. Of these standard systems, Bluetooth 5.1 is the one capable of positioning with centimeter accuracy, but the range of technology does not allow stable operation in an industrial-scale environment. The most commonly known radio frequency positioning generally uses the Received Signal Strength Indication (RSSI) method, which determines the position of the devices by triangulation based on the strength of the detected signals [23]. However, these measurement procedures are unreliable in terms of accuracy. The exact positioning can be solved by the so-called Angle of Arrival (AoA) and Angle of Departure (AoD) measurement procedure shown in Figure 4. The essence of AoA is that the transmitter device first uses a single antenna to send a directional data packet that the receiver detects with multiple antennas. The system algorithms calculate the arrival angle and direction of the signal based on the minimal delay the packets arrive with to the antennas.

AoD is the opposite of AoA. Here, a sending device works with several antennas, from which it simultaneously sends signals to the receiver with one antenna, for positioning purposes. The signals arrive at the receiver with a delay, so an algorithm can calculate the direction from which the received signal was received. This principle is the most similar one to satellite positioning. The clearer the view of the transceivers and receivers, the more accurately the technology works. Objects and walls in the path may cause interference, impairing accuracy [24].

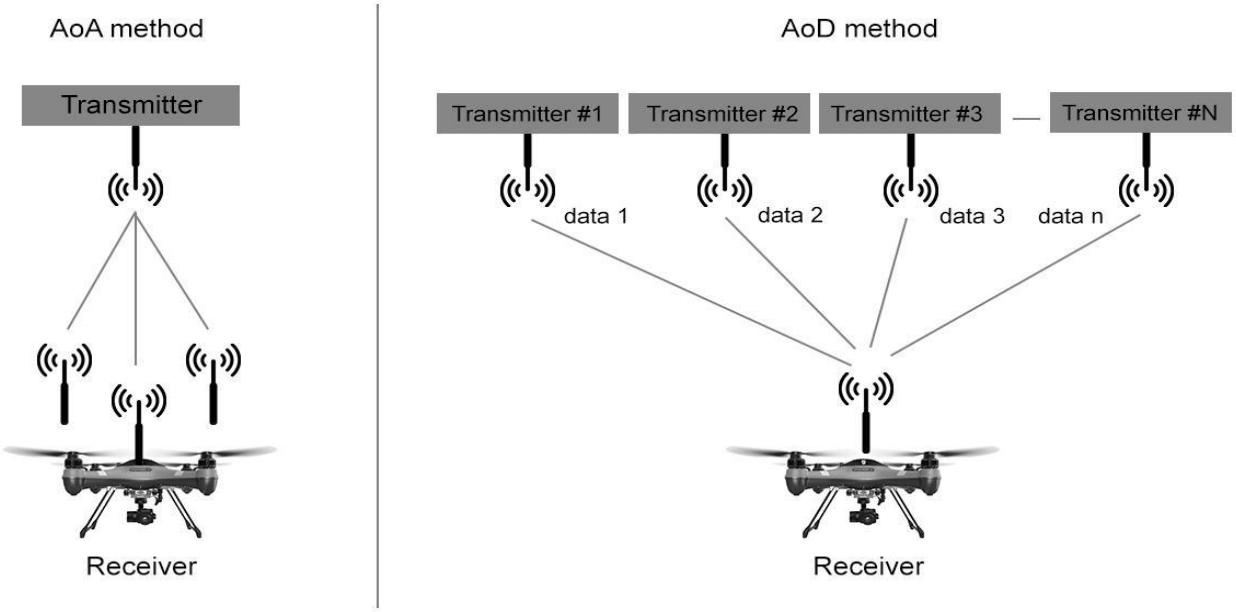

Figure 4. AoA and AoD system positioning.

Systems for flight support and data acquisition

The drone sensor system assists in the safe execution of tasks, both indoors and outdoors. To achieve this goal, it is necessary to create a hardware and software environment that is responsible for flight planning - determining routes, turning points, and altitude. The system is able to stay in constant communication. With the help of an operator, a so-called work management option can be implemented, which ensures that the flight plan is modified on the move. The operator can track the changes and the current position of the drones on a properly designed graphical interface. It also makes it possible to monitor drone sensor data - eg. distance detection, speed, charge level, flight altitude. In these systems, the data is processed continuously, so that the operator can be informed about the measurement results even during the task completion, and, if necessary, can intervene manually.

CONCLUSION

The drones need to become smarter in order to optimize industrial processes, maximize their utility and be widely accepted in future factories. If all these criteria are realized, they can be applied in engineering, maintenance, critical infrastructure management, and asset management operations. The use of drone systems in the industry clearly offers new opportunities and new innovative business models. To accelerate manufacturing processes, companies are trying to implement these new innovative technologies into their systems to make their processes safer, more reliable, and more predictable. The drones appear as a new alternative in this area (eg.: swarms of autonomous drones). From an industry standpoint, the implementation of this technology can be ideal in the automotive industry. This is projected by test plants in car parts manufacturing (eg Subi-Ker 2000 Ltd. factory and innovation center) [25-30].

ACKNOWLEDGEMENT

The research on which the publication is based has been carried out within the framework of the project entitled “Újszerű biztonsági megoldásokkal rendelkező kis teherbírású univerzális – A low-capacity universal cobot system with innovative safety solutions”, application number GINOP-2.1.2-8-1-4-16-2018-00492.

REFERENCES

[1] Mester, Gy. 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,

[2] Mester, Gy. and Rodic, A.: *Simulation of quad-rotor flight dynamics for the analysis of control, spatial navigation and obstacle avoidance.*
In: *3rd International Workshop on Advanced Computational Intelligence and Intelligent Informatics*, IWACIII, 2014,

[3] Lazányi, K.: *Stressed Out by the Information and Communication technologies of the 21st Century.*
Science Journal of Business and Management **4**(1-1), 10-14, 2016,
http://dx.doi.org/10.11648/j.sjbm.s.2016040101.12,

[4] Lazanyi, K.: *Readiness for Artificial Intelligence.*
In: *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics, SISY*. IEEE, Subotica, 2018,
http://dx.doi.org/10.1109/SISY.2018.8524740,

[5] Hajdu, B. and Lazányi, K.: *Trust in human-robot interactions.*
In: *2017 IEEE 14th International Scientific Conference on Informatics*. IEEE, Poprad, 2017,
http://dx.doi.org/10.1109/informatics.2017.8327249,

[6] Mezei, J.I. and Lazányi, K.: *Are We Ready for Smart Transport? Analysis of Attitude Towards Public Transport in Budapest.*
Interdisciplinary Description of Complex Systems **16**(3-A), 369-375, 2018,
http://dx.doi.org/10.7906/indecs.16.3.9,

[7] Lazányi, K.: *Are we Ready for Self-Driving Cars-a Case of Principal-Agent Theory.*
In: *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics, SACI*. IEEE, Budapest, 2018,
http://dx.doi.org/10.1109/saci.2018.8441011,

[8] Amza, C.G., et al.: *Guidelines on Industry 4.0 and Drone Entrepreneurship for VET students.*
In: Danmar Computers, Drone technology training to boost EU entrepreneurship and Industry 4.0, pp.1-45, 2018,
http://ludoreng.com/eduDrone/IO2_eduDrone_EN.pdf,

[9] Fernández-Caramés, T.M.; Blanco-Novoa, O.; Suárez-Albela, M. and Fraga-Lamas, P.: *A UAV and Blockchain-Based System for Industry 4.0. Inventory and Traceability Applications.*
In: *5th International Electronic Conference on Sensors and Applications*. MDPI, 2018,
http://dx.doi.org/10.3390/ecsa-5-05758,

[10] Patterson, J.: *An Aerial View of the Future – Drones in Construction*
Geospatial World, 2018.
https://www.geospatialworld.net/blogs/an-aerial-view-of-the-future-drones-in-construction, accessed 5th May, 2018,

[11] Nemes, A. and Mester, Gy.: *Unconstrained evolutionary and gradient descent-based tuning of fuzzy-partitions for UAV dynamic modeling.*
FME Transaction **45**(1), 1-8, 2017,
http://dx.doi.org/10.5937/fmet1701001N,

[12] Rubóczki, E.Sz. and Rajnai. Z.: *Moving towards cloud security.*
Interdisciplinary Description of Complex Systems **13**(1), 9-14, 2015,
http://dx.doi.org/10.7906/indecs.13.1.2,

[13] Tokody D.; Albini, A.; Ady, L.; Temesvári Zs.M. and Rajnai, Z.: *Kiberbiztonság az autóiparban.*
Bánki Közlemények **1**(3), 71-77, 2018,

[14] Illési, Zs.: *Cyberterrorism from IT Forensics Perspektive.*
Magyar Rendészet **13**, 55-62, 2013,

[15] Berek, L. and Vass, A.: *Transzformátor állomás szállítása közúton.* Hadmérnök **12**(3), 76-90, 2017,
[16] Vass, A.; Maros, D. and Berek L.: *Veszélyhelyzeti infokommunikáció az energetikai black out alatt.* Bólyai Szemle **24**(2), 63-76, 2015,
[17] Iantovics, L.B.; Gligor, A. and Georgieva, V.: *Detecting Outlier Intelligence in the behavior of intelligent coalitions of agents.* In: 2017 IEEE Congress on Evolutionary Computation (CEC). IEEE, San Sebastian, 2017, http://dx.doi.org/10.1109/MCI.2017.2742840,
[18] Nahangi, M.; Heins, A.; McCabe, B. and Schoellig, A.: *Automated Localization of UAVs in GPS-Denied Indoor Construction Environments Using Fiducial Markers.* In: 35th International Symposium on Automation and Robotics in Construction. The International Association for Automation and Robotics in Construction, Berlin, 2018,
[19] Kasac, J.; Milic V.; Stepanic, J. and Mester, Gy.: *A computational approach to parameter identification of spatially distributed nonlinear systems with unknown initial conditions.* In: 2014 IEEE Symposium on Robotic Intelligence in Informationally Structured Space, RiiSS 2014. IEEE, Florida, 2014, http://dx.doi.org/10.1109/RIISS.2014.7009170,
[20] Cveticanin, L.; Mester, Gy. and Biro, I.: *Parameter influence on the harmonically excited Duffing oscillator.* Acta Polytechnica Hungarica **11**(5), 145-160, 2014,
[21] Khosiawan, Y., et al.: *Task scheduling system for UAV operations in indoor environment.* In: Neural Computing and Applications, Springer London, 2018, http://dx.doi.org/10.1007/s00521-018-3373-9,
[22] Khosiawan, Y. and Nielsen, I.: *A system of UAV application in indoor environment.* Production & Manufacturing Research **4**(1) 2-22, 2016, http://dx.doi.org/10.1080/21693277.2016.1195304,
[23] Kiss Leizer, G.K. and Tokody, D.: *Radiofrequency Identification by using Drones in Railway Accidents and Disaster Situations.* Interdisciplinary Description of Complex Systems **15**(2), 114-132, 2017, http://dx.doi.org/10.7906/indecs.15.2.1,
[24] Hell. P.; Mezei, M. and Varga, P.J.: *Drone communications analysis* In: SAMI 2017, IEEE 15th International Symposium on Applied Machine Intelligence and Informatics. IEEE, Budapest, 2017,
[25] Sören, K.: *Autonomous logistic systems for smart factories.* Robotics for Logistics and Transport -ERF 2016 Workshop,1-12, 2016. http://web.itainnova.es/eurobotics/erf-2016-workshop-robotics-for-logistics-and-transport, accessed 7th May, 2019,
[26] Bocchetti, G.; Flammini, F.; Pragliola, C. and Pappalardo, A.: *Dependable integrated surveillance systems for the physical security of metro railways.* Third ACM/IEEE International Conference on Distributed Smart Cameras. IEEE, Como, 2009, http://dx.doi.org/10.1109/ICDSC.2009.5289385,
[27] Flammini, F.; Setola, R. and Franceschetti, G.*: Effective Surveillance for Homeland Security.* Taylor & Francis Group, New York, 2013,
[28] Iantovics, L.B.; Emmert-Streib, F. and Arik, S.: *MetrIntMeas a novel metric for measuring the intelligence of a swarm of cooperating agents.* Cognitive Systems Research **45**, 17-29, 2017, http://dx.doi.org/10.1016/j.cogsys.2017.04.006,
[29] Pető, R.: *Drone's safety and security questions I.* Hadmérnök **11**(4), 150-158, 2016,
[30] Pető, R.: *Some Safety and security issues of UAVS.* Acta Technica Corviniensis – Bulletin of Engineering **2017**(3), 55-60, 2017.

Interdisciplinary Description of Complex Systems 17(3-A), 468-475, 2019

POSSIBLE SMART CITY SOLUTIONS IN THE FIGHT AGAINST BLACK ECONOMY

Piroska Dobos[1], * and Katalin Takács-György[2]

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

[2]Óbuda University, Faculty of Business and Management
Budapest, Hungary

DOI: 10.7906/indecs.17.3.5
Regular article

Received: 11 December 2018.
Accepted: 31 August 2019.

ABSTRACT

According to international statistics, Hungary has a high ratio of black economy. On December 31th of 2017, the number of registered corporations reached 1.7 million, of which 395 910 were registered in Budapest [1]. There is a clear need for such measures and developments that are aimed to track corporations at the e-government level, and such infocommunicational equipment and services that essentially promote the arrangement of data. Black employment is one of the most easily identified territories of the hidden economy. Employers must register the working hours, and they are also responsible for the factual, real and entire content of the registry. A number of entry systems are available which – besides ensuring electronic protection – are also suitable for registering the working hours. These systems, however, have both advantages and disadvantages, and different types of abuses have become widespread. The purpose of the study is to provide an overview of these systems based on their ability to reduce black employment and the limitations of their applicability from the point of data protection, with particular attention to the introduction of the General Data Protection Regulation of the European Union from 25 May 2018 in all member states. Employers manage data through their legitimate interest on web and telephone usage, control of emails, or even GPS-based location information. Likewise, legitimate interest is also the basis of the introduction of workplace monitoring systems. To reduce the size of the black economy, the use of an electronic system would be the most suitable tool – which would transfer the information extracted from the system to an immediate tax authority – based on the patterns of online cash registers or online billing programs. This, on the one hand, could provide the basis for the necessary identification and work documentation, but on the other hand, it raises the risk of excessive data handling, which is illegal.

KEY WORDS

hidden economy, black employment, access control systems, security solutions, e-government

CLASSIFICATION

JEL: H26

*Corresponding author, η: d.piri@globalprofit.hu; +36 70 456 1812;
OE-BDI office, Nepszinhaz str. 8, 1081 Budapest, Hungary

INTRODUCTION

As a result of accelerating urbanization, our cities have to face new challenges. Smart city theories are searching for solutions to the challenges of the present age, using the tools of the present age, primarily through the use of infocommunication technologies. The key objective of a smart city is to improve the efficiency and effectiveness of city operations. In addition, improving the quality of life of the citizens and raising the standard of living are significant aspects as well, in a way that remains respectful towards natural resources. The main rating indicators used by city rating agencies are primarily technology, economy, governance and politics, as well as human, social and environmental issues. In Europe, Hungary is unfortunately among the last countries on the list next to Romania and Bulgaria. In many respects, the economic factor is one of the most important part of the smart city system. The performance of the economy plays a key role both in measuring effectiveness and in financing technological innovations. Smart economy is based on productivity, the adoption of new and developing industries. Its fundamental goal is to ensure a skilled workforce and to create the highest extent of flexibility in the labour market. Governance and the political segment are also important factors in the smart city initiative. The aim is to create an administrative sphere that can, through the use of infocommunication technology, create a cooperative, transparent office system. Widening the sphere of services and improving their accessibility and integrity greatly promote the development of society integration. An important goal is to reduce bureaucracy and increase the role of responsibility. The role of the e-administration system should also be emphasized in this field. Extending a number of services, such as a unified register, the development of healthcare and the reduction of administrative burdens substantially increase the quality of life of smart city citizens, while these innovative solutions at hand improve the standard of living [2].

The hidden economy is a very complex economic phenomenon. It can be detrimental to the real, so-called "white economy". Hidden economies require increasing attention due to their internal dynamics, and their operation requires coordinated responses both at national and international levels. Based on the results of his international comparisons, F. Schneider – one of the most prestigious researchers of the "shadow economy" – quantified the presumed ranking of the hidden economy of countries in the world. According to the survey, in the developing countries, the size of the hidden economy (expressed as a percentage of the official GDP) was 19,8 %, in Eastern and Central Asia (transition countries) 38,1 %, while in the OECD countries 18,7 %. In the specific rankings, Hungary is ranked 44th, while in the 21 transition countries it is ranked 3rd with a 25,8 % of the GDP order of magnitude [3]. These activities make it impossible to determine the real economic performance of economic operators, which leads to a deterioration in the tax morale, and as a natural result, the budget receives less revenue. Its ethical effects cannot be neglected either, as they act against the basic rules of free market economy and also against free competition. Revenues from hidden economic activities can upset the balance between the economy, politics and even the armed organizations, which may lead to the destabilization of a country or a whole region [4]. Combating the hidden economy and its scale is an important political objective for all countries. Corruption is similar everywhere in the world, in all political-economic systems, to a lesser or greater extent [5], but the present study is not intended to examine this problem.

CONSEQUENCES

The ratio of black economy in Hungary is high compared to international practice. One of the well-identified areas of the hidden economy is black employment. An important step in the tax behaviour of companies is the decision to declare and pay labour-related taxes and

contributions. Due to tax evasion and tax avoidance, the validity of the companies' income data can be questioned at several points. Both the actual number of the formally employed and declared staff and the wages actually paid to them are questionable. In both cases, actual labour costs are different from those calculated formally and statistically based on tax declarations. The validity of the headcount data can be questioned at two points. One typical practice in the hidden economy is the employment of undeclared workforce and the handing over of the payment in cash, without any documentations. In this case, both the company, and the black employee commit tax evasion. It may also be a case of tax evasion, when employee person acts permanently as a subcontractor, with its own company or enterprise [6]. Within the framework of black employment, the most commonly used methods include the employment of undeclared employees, the pretence of a legal relationship or a simulated business contract, and the employment at a minimum wage. Each method significantly reduces the budget payment obligations. For this reason, there is a need for a number of steps to be taken in this area.

When Hungary joined the European Union, a new, uniform labour database was introduced (EMMA), which obliges all employers to register their employees. The EU and OECD guidelines are regularly reviewed and considered in Hungary [4]. These policy approaches can take the form of tax measures, direct, fiscal measures, work regulations, and other applied interventions or government measures. Government measures include the enforcement of laws and the identification of violators. The classic way of reducing the hidden economy is to increase the severity of punishment. This solution seems fairly obvious and is widely used. Fines and other applicable measures in case of the employment of undeclared employees are specified in the Act on Taxes.

The taxpayer must be subject to a default penalty of up to HUF 1 million when employing or if employed as an undeclared employee. In addition to imposing default fines, the tax authority may close the premises of the taxable activity for 12 opening days if the taxpayer is employing an undeclared employee. In case of a repeated violation the closure period is 30, and in every additional cases 60 days of opening. The room is sealed with a tax authority stamp, clearly indicating the termination period and the fact that the business was closed by the tax authorities. In the event of blocking the closure, the tax authorities may use the police to cooperate, according to the provisions of Sections 170-174 of the Art Act [7]. This visible action obviously causes not only financial damage to the taxpayer, but also a significant loss of prestige, which can lead to further material damages. In addition, according to Section 82 of the Ávr, the National Taxation and Customs Authority (NAV) continuously publishes the name, registered seat and tax number of those taxpayers on its website who have not fulfilled their obligation to report the establishment of an employment relationship [8].

DECLARATION OF EMPLOYEES, WORKING HOURS REGISTER

According to Section 16 of the Art, the employer must report the employee to the tax authority before the beginning of the employment, if he establishes a new insurance relationship, i.e.: at the beginning of the insurance, at the latest on the first day of the insurance relationship before the start of the employment [7]. The proper keeping of the working time records is the duty of the employer and therefore it is responsible for keeping the records factual, true and complete. The records kept by the employer must comply with the requirements of completeness, verifiability, updating and credibility, while it also has to be found at the place of work. Under Section 134 of the Labour Code, the employer must record normal and extraordinary working hours, duration of standby and leave. The register must also be able to keep the normal and extraordinary working hours and the start and end times of the standby up to date [9].

The access control systems represent one of the key areas of security electronics. Their primary purpose is that entering and residing in a given area can only take place by authorized persons. Access to different parts or areas within the objects can be separately restricted. Thus, the access control system basically regulates, but the owner and operator of the object have the possibility to use other services of the system, such as the work time register already mentioned. First, the access control system has three main functions. Identification of the entry entitlement and identification of the persons entering the passage control. Of course, the archiving and storage of events are a key function of the system as well as logging. The basic elements of the access control systems are access points installed at the entrances of the objects, premises and areas that are connected to a computer centre via the local communication network at online systems. This centre should be able to make complex choices regarding the number of persons, the eligibility of persons in the given audited space, the existence of the rights related to the tasks to be performed (the qualification of certain persons as above) requires a joint assessment of the signals from the sensors reporting the functionality of the technical equipment to ensure the operation of the facility [10].

Electronic work time recording systems are also suitable for reducing black employment, however these methods have disadvantages as well (Table 1). For these systems, it is very important that the logging data cannot be retrofitted so that they can provide stable, retrospective, analytical records for payroll and contribution disclosure. The knowledge-based identification methods are best known for password-based authentication. The disadvantage of this method may be that employees can easily pass on passwords to each other, so this can give rise to abuse, as it cannot be identified whether the password was given by the employee who really owns it or by someone else In this method, no physical presence is required from the employee; a single person can enter several codes, while the others are not actually present. Data is electronically logged when the employee is identified. It is also important to pay attention to the correct password selection so that the password cannot easily be guessed. In addition, it is also important to have adequate data protection, that is, the correct storage of the sample patterns used for comparison, so that unauthorized persons cannot access it. It is advisable to increase the protection by changing passwords from time to time.

In the case of possession-based identification, the use is generally simple, and there are rather cheap and relatively expensive solutions as well. It is safer than password-based authentication, because the card needs to be passed in order to register for someone else, but it still does not provide protection against pre-planned fraud, as the card previously delivered can be validated by someone else than the actual cardholder, since it is the card that is identified and not the specific person. Thus, if an unauthorized person gains possession, unauthorized access is possible.

However, biometric identification is becoming a key element today, whether it means fingerprint reading, vein-network scan, retinal scan or face recognition. It has a wide range of uses, which can be found everywhere from access, through the registration of working hours to the unlocking of mobile phones. Biometric features are unique to every person, and such identification is very reliable, efficient, and convenient. The risk of abuse is much smaller in size than in the case of cards (stolen or borrowed cards are a known problem). Combining multiple identification methods (two- or three-level identification) further reduces abuses. In contrast to knowledge and possession-based identification, here it is the person him-or herself who is identified. Each biometric system is based on biometric patterns or templates that are collected in advance and then used for comparison later. There are two basic ways to handle biometric patterns. The first is to store the samples in a database or in the reader memory. The second uses ID cards to store unique patterns. Naturally, this method may have disadvantages as well. These systems are fairly expensive. For this reason, they have not been

Table 1. Advantages and disadvantages of working hour register systems.

REGISTER	CHARACTERISTICS
Paper based attendance sheet	it is very easy to falsify, fill in afterwards
	lacks any automatism or "intelligence"
	its accuracy is largely influenced by human neglect
	the time of entry is not logged, so it can be filled in at any time
Working hours recording by a dispatcher or a gatekeeper	human interaction is still high, but the person making the entry is different
	friendships, hostilities can be enforced in the system
	the time of entry is not logged either
Electronic working time recording systems	
Knowledge-based identification	the employee can identify him or herself with a code or password
	codes and passwords can easily be passed on to each other
	it cannot be made sure that the employee be there in person
	no physical presence is required from the employee
	one person can use more codes while the others are not present
	it is electronically logged
Possession-based identification	a proxy card or some other device is possessed by the employee
	it is safer than knowledge-based, because the card needs to be handed over
	it still lacks protection against pre-planned fraud
	here too, it is the card that is identified, and not the real person
Feature-based identification	such as biometrics, where, for example, the fingerprint can be used for identification
	the safest system, the employee has to be present here
	a suitable biometric system should be chosen for the right place
	high price
Modern mobile solutions	it is a mobile application and registration is carried out through these
	modern, emerging solutions
	they are not too widespread, very little experience is available
	through the phone it is easy to handle the start of working time and holidays
	can be optimal for non-stationary workers (GPS)

widely used to record working time or to facilitate payroll, but there may be a number of areas or industries where they need to be introduced because of high security requirements which demand the biometric entry of the employees, and where the differentiation between employees and non-employees may only be made this way. Nevertheless, this conclusion must be based on an individual examination in each case [11].

LIMITATIONS OF THE APPLICABILITY OF THE ACCESS SYSTEMS – DATA PROTECTION

The employer is entitled to monitor the work of the employees and their fulfilment of other labour law obligations as a result of the employment relationship. This right is also ensured

by the Labour Code. However, this monitoring is limited by the personal data rights of the worker concerned, which includes the right to protect their personal data. Until recently, the field of data protection had been defined in Hungary by state regulations. It is worthwhile for the employer to consult the provisions of the Act on informational self-determination and freedom of information when implementing a registration system [12]. However, this framework-based directive has been replaced by a regulation of the European Union that is uniformly applicable in all countries in order to create a single internal market. The General Data Protection Regulation of the European Union (Regulation No 2016/679 or GDPR) [13] has already been in force for two years but it has only been applicable in all Member States from 25th May, 2018. These rules are accompanied by unprecedented penalties. The difficulty is further enhanced by the fact that under the new rules the SME sector will not be exempt in any area. Personal data may only be dealt with for a specific purpose, for the exercise of rights and for the fulfilment of obligations. At all stages of data management, the purpose of data management must be appropriate and the recording and handling of data must be fair and legitimate. In addition, only those personal data that are essential for achieving the purpose of data management can be handled to achieve this goal. Personal data can only be handled to the extent and for the duration required to achieve the goal. For example, the use of biometric technology in different countries is regulated differently. It is therefore important to know the local regulations prior to making biometric technology decisions. At the same time, it is necessary to observe the purpose-bound data handling principle, to consider the obligation of data-minimalisation, and in case of several identical data management methods, to choose a method that least restricts the rights of the affected persons or that does not include employer data management. Because of these requirements, for the purpose of payroll and working hours control, the use of biometric data is not the most suitable solution.

The basic rule of data protection is that the employee must always be informed of all circumstances. Under Section 10 (2) of the Labour Code, the employer is obliged to inform the employee of the handling of his/her personal data. In addition, the employer may disclose any facts, data, and opinion about the employee to a third party only in cases specified by law or with the employee's consent. One exception is the forwarding of personal data towards a data processor. For the purpose of fulfilling the obligations arising from the employment relationship, the employer may transfer the employee's personal data to the data processor, for example, to the accountant, by indicating the purpose of the data supply, as defined by law. However, the employee must be informed in advance; therefore the transfer of data should be included in the policy. The employer may also monitor the employee in his/her employment relationship. If the employer exercises the right of monitoring, he or she must previously inform the employee of the application of the technical means for monitoring. The legitimate interest of the employer is the main legal basis for data processing at work. This is an important facilitator for the employer, which includes for example the checking of web-use, phone calls or e-mails, or even GPS-based positioning. Similarly, this lawful interest provides basis for the use of workplace surveillance systems, which must meet various other conditions.

CONCLUSIONS

In conclusion, besides being able to reduce black employment, a good system must meet the following requirements: it must ensure that the person is fully identifiable, the beginning and the end of working time is logged; and neither the employee nor the employer could modify the data and the automatism of evaluation of reports and offenses. There are various methods available for time recording, each having their advantages and disadvantages, and different degrees of misuse. To reduce the size of the black economy, the use of an electronic system would be the most suitable tool – which would transfer the information extracted from the system to an immediate tax authority – based on the patterns of online cash registers or online

billing programs. However, this raises a number of issues, including the cost requirements of different systems, the extent of which may not necessarily be passed on to all business sizes. Also, it must not be forgotten that various legal questions and data protection issues may arise. Before the introduction of a system – from a data protection perspective - a so-called 'interest-weighing' test should be carried out, in which the legitimate interests of the employer must be examined, the interests of the workers concerned must be identified, consideration must be given to the individuals' rights and interests, a necessity-proportionality test must be performed and the result of these must be brought to the attention of the data subjects. Otherwise excessive data handling might occur, which is illegal. Considering the observation of the principles of Article 5 of the GDPR, personal data must be handled only to such extent that is actually required to ensure the rights and obligations originating from the labour relationship. Certain data management operations, even with the employee's consent, may raise concerns. For example, an examination of work by an electronic system, or the use of photo IDs at work (access card, email photo ID, etc.).

Despite the fact that the tax policy remains the most obvious means to enforce tax payments, or the policy of deterrence, which implies that greater fines and penalties result in better enforcement, it can have an opposite effect on the side of taxpayers. The enforcement efforts can increase tax compliance, but extreme punishments can be counterproductive as they might result in lower tax payments and in a loss of confidence in state institutions [14]. The government and public administration can reduce the tax rate and the intensity of regulation, but it also has to strive to achieve socially optimistic rates of taxation and regulation. Therefore, it can be stated that there is an optimal degree of hidden economy in every economy, where it is not worth increasing or further reducing the fiscal expenditures on tax audits.

REFERENCES

[1] STADAT: *Number of registered enterprises (2013-2017).*
http://www.ksh.hu/docs/hun/xstadat/xstadat_evkozi/e_qvd017c.html, accessed 2nd December 2018,

[2] Szendrei, Zs.: *Smart city, the city of the future*.
http://www.urb.bme.hu/segedlet/varos1/eloadasok_2014/07B_SMART%20CITY_SZENDREI%20ZSOLT_kivonat.pdf, accessed 2nd December 2018,

[3] Schneider, F.; Buehn, A. and Montenegro, C.E.: *Shadow Economies All over the World: New Estimates for 162 Countries from 1999 to 2007.*
Policy Research Working Paper, 2010,

[4] Belyó, P.: *The emergence of the hidden economy as a result of new economic policy practices.*
XXI. Century – Scientific Publications 27, 2012,

[5] Takács, I.; Csapodi, P. and Takács-György, K.: *Corruption as a deviant social attitude.*
Public Finance Quarterly **2011**(1), 27-43, 2011,

[6] Semjén, A.; Szántó, Z. and Tóth, I.J.: *Tax fraud and tax administration, Microeconomic models and empirical analysis of the hidden economy.*
Budapest, 2001,

[7] –: *Act XCII of 2003 on the Rules of Taxation.*
https://net.jogtar.hu/jogszabaly?docid=A0300092.TV&timeshift=20160801&txtreferer=A1000185.TV, accessed 2nd December 2018,

[8] –: *Government Regulation no. 368/2011. on the Implementation of the Act on Public Finances.*
https://net.jogtar.hu/jogszabaly?docid=A1100368.KOR, accessed 5th December 2018,

[9] –: *Act I of 2012 on the Labor Code.*
https://net.jogtar.hu/jogszabaly?docid=A1200001.TV, accessed 5th December 2018,

[10] Berek, L.; Berek, T. and Berek, L.: *Personal and property security*.
Óbuda University, Budapest, 2016,

[11] Dobos, P. and Kiss, S.: *The fight against black employement – possible security solutions.* Hadmérnök **13**(2), 9-16, 2018,

[12] –: *Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.* https://net.jogtar.hu/jogszabaly?docid=A1100112.TV, accessed 5th December 2018,

[13] –: *Regulation (EU) 2016/679 of the European Parliament and of the Council.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=HU, accessed 5th December 2018,

[14] Dobos, P. and Takács-György, K.: *Measurement possibilities of motivations and attitudes influencing the formation of unethical business behavior – the effect of self-esteem on the black economy.* In: Szikora, P., ed.: 16th International Conference on Management, Enterprise and Benchmarking. Óbuda University, Budapest, pp.92-106, 2018.

Interdisciplinary Description of Complex Systems 17(3-A), 476-484, 2019

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].

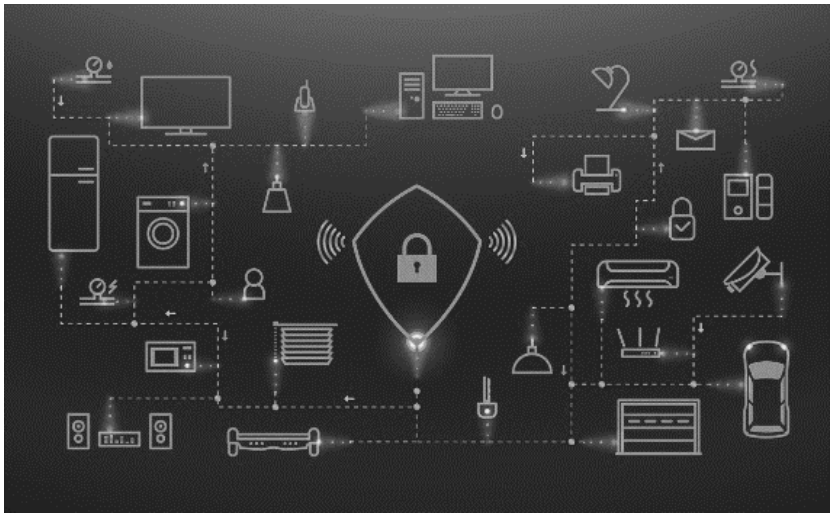

Figure 1. IoT devices [3].

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:

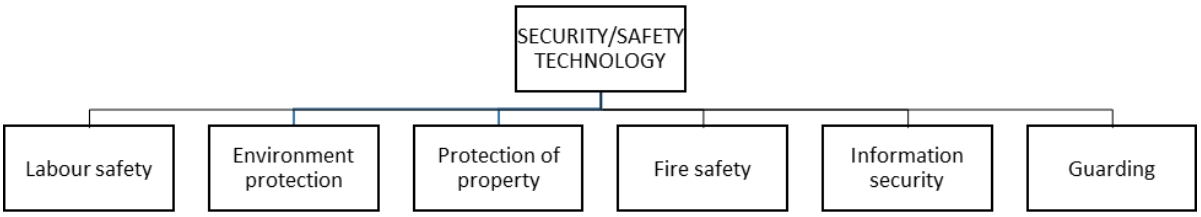

Figure 2. Areas of security technology.

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.

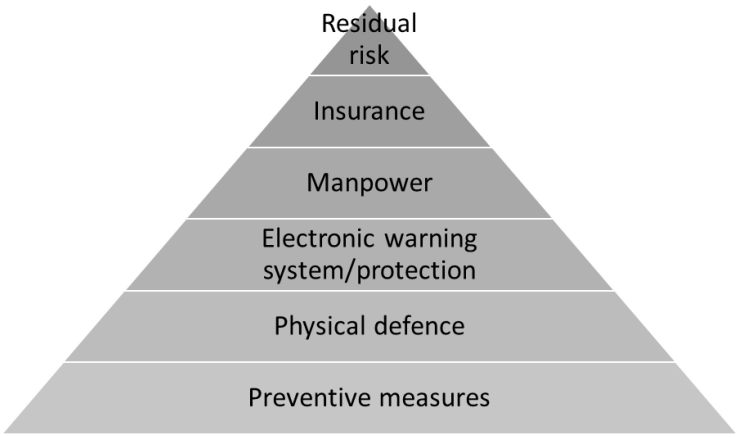

Figure 3. Steps of establishing security/safety (Security Pyramid) [18; p.13].

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).

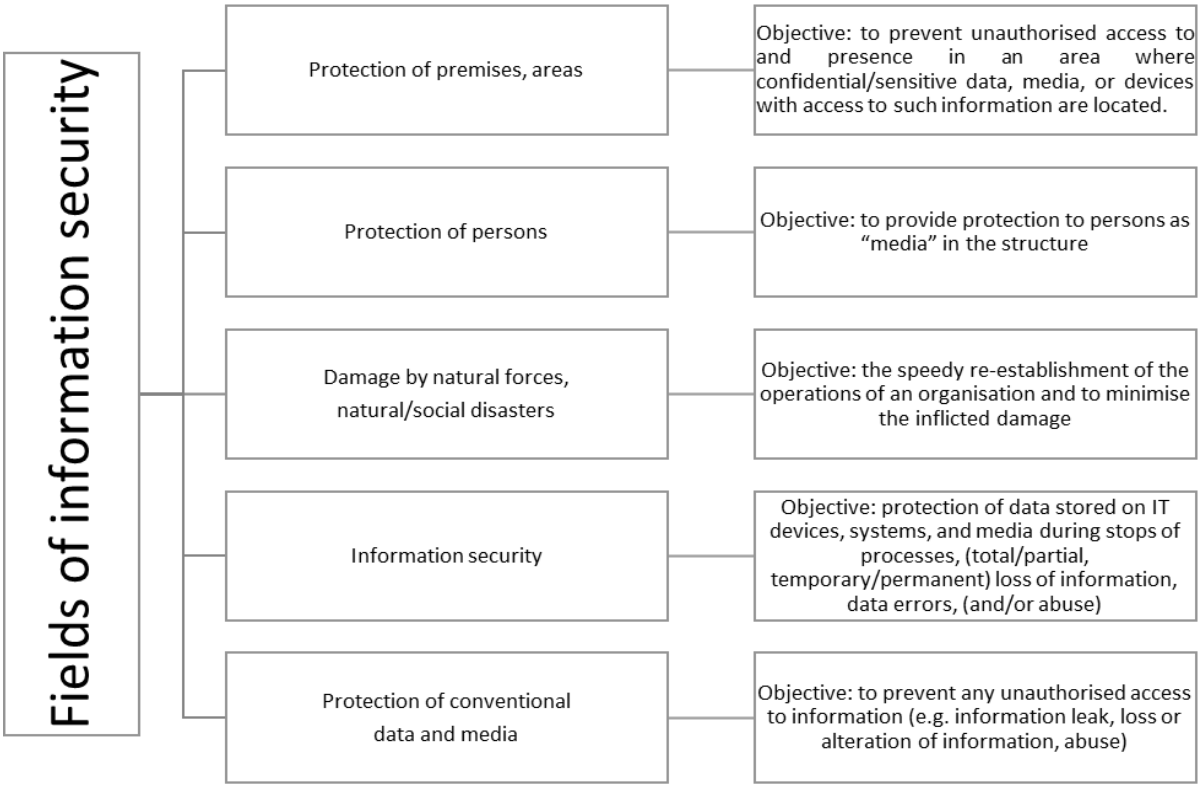

Figure 4. Areas for implementing information protection procedures [19].

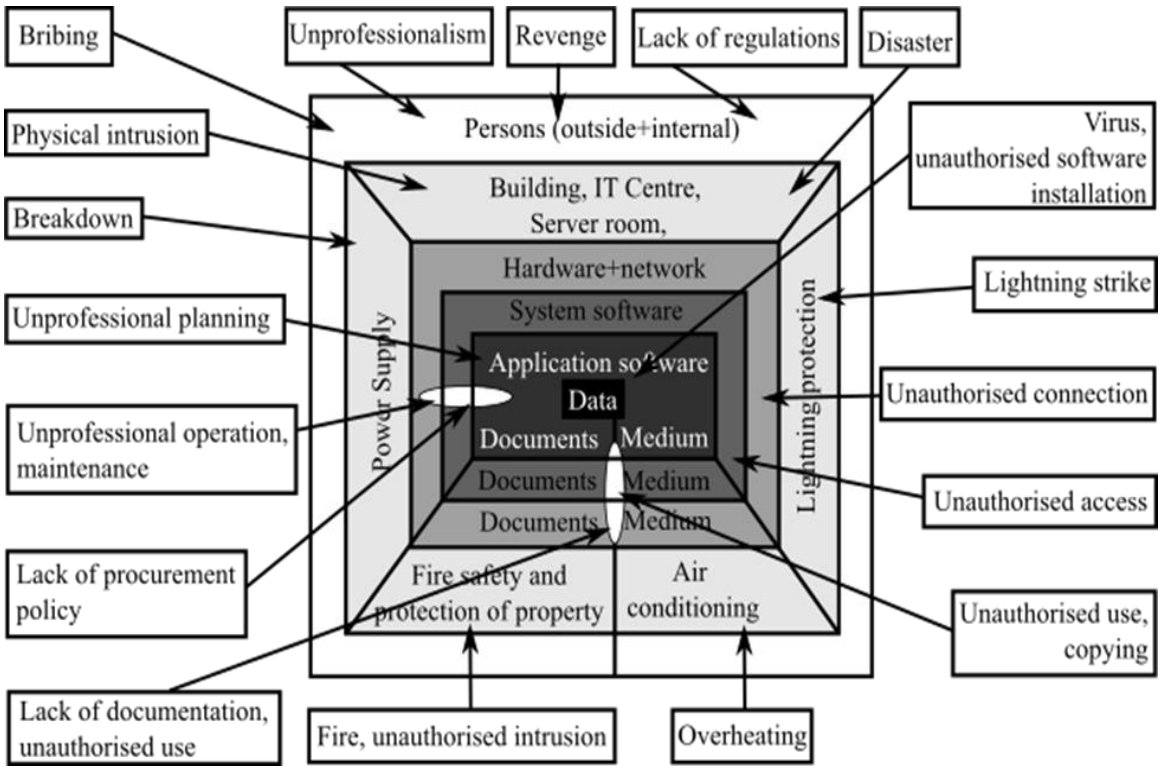

Figure 5. Example of grouping threats [20; p.33].

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.

Interdisciplinary Description of Complex Systems 17(3-A), 485-491, 2019

PARAMETERS AND GUIDELINES OF ENFORCEABLE INFORMATION SECURITY MANAGEMENT SYSTEMS

Sándor Dombora*

[1]Óbuda University, Kandó Kálmán Faculty of Electrical Engineering
Budapest, Hungary

DOI: 10.7906/indecs.17.3.7
Regular article

Received: 8 December 2018.
Accepted: 31 August 2019.

ABSTRACT

It is increasingly important for organizations to set up an Information Security Management System (ISMS) to fulfil their business interests and their legal compliance. The main purpose of these systems is to properly protect the information owned or managed by the organization. Often, the developed ISMS complies with the external regulatory environment, but contains unenforceable rules that impede work, so it is unable to fulfil its function. In order to prevent security incidents, it is not enough to ensure legal compliance. The enforceability of these policies is gaining increasing importance in order to avoid hindering work processes. This article identifies quality parameters and guidelines in order to improve quality, enable and improve enforceability of ISMS systems, in order to fulfil their purpose, mainly protection of company information assets. By adhering to these parameters and guidelines organisations can improve their ISMS systems which enforces security of their information assets.

KEY WORDS

information security, quality parameters, implementation directives, enforceable measures

CLASSIFICATION

ACM K.6.5
JEL: D83

*Corresponding author, η: dombora.sandor@kvk.uni-obuda.hu; +36 1 666-5140;
Institute of Communication Engineering, Kandó Kálmán Faculty of Electrical Engineering, Óbuda Univeristy, H – 1084 Budapest, Tavaszmező u. 15-17. Hungary

INTRODUCTION

Organizations collect, store and process a large amount of information to achieve their goals. Several companies gather more information than necessary to run their business operations. The information is collected, stored, accessed and processed by employees. The collected information is not only valuable for the organisation but for the competitors too. In some cases, the information may be interesting for a larger public as well. The data may contain confidential information, leakage of which may cause harm not only to the organisation but to partners, users and customers too.

The information processed by organisations can be grouped by different categories. Enterprises deal with information about: products, production, personnel, customers, partners, rules and regulations, workflows, design and development, research, quality management, organisation structure, business reports, etc. information.

Depending on the nature of the information, the legal environment may require the development of security policies and regulations, as well as the implementation of security measures. For example, personal data are protected by law everywhere in the world. First, however, the meaning of personal data must be specified. The term is defined by the law applicable in each geographic region. For example, in the European Union the meaning of personal data is defined by the General Data Projection Regulation (GDPR) [1], which may be complemented by the local laws of the EU member states.

Depending on the nature of the information collected, stored and handled by the organisations, it should be protected according to the business needs and the legal environment. Several factors govern the data protection needs of an organisation. The most important ones are the following:

- supporting production with availability of authentic information,
- ensuring information integrity to improve productivity and quality [2],
- avoiding fines, caused by law breaches (GDPR [1], sectoral legislation, Act CXII of 2011 on Information Self-Determination and Freedom of Information [3], Hungarian Act L of 2013 on Electronic Security of State and Local Government Bodies [4], etc.),
- ensuring the protection of sensitive information,
- management reports based on authentic data,
- using the market advantage of the ISO/IEC 27001 certification [5].

To achieve these goals, organisations need a functioning and enforceable ISMS. Articles describing the modelling of ISMS parameters have been identified [6], and the quality improvement based on ISO27000 has already been presented [7]. Other authors refer to the information security aspects related to process resource planning [8] and IT authorisation and Identity management [9]. These works suggest a need for an ISMS quality parameter and guidelines set to help organizations set up an operating ISMS system.

To further improve information security, this paper identifies a set of parameters and guidelines whose application greatly improve the quality and enforceability of ISMS.

RESEARCH METHOD

To identify quality parameters and guidelines for ISMS action research approach was used [10].

The first step of the research was to identify and categorize the problems which block enforcement of ISMS.

The second step was to define quality parameters and development guidelines to avoid building unenforceable ISMS. The result was a set of guidelines to follow and quality parameters to build into ISMS during development.

The third step was the implementation of an ISMS based on the developed guidelines and quality parameters in a large organisation which had several, smaller, loosely coupled subsidiaries with different information security needs.

In the last step, the developed guidelines and quality parameters were used to build several ISMS at different organisations. After a year of the ISMS implementation, these organisations were visited and interviews were made with stakeholders about the achieved result, which gave feedback and helped to improve the development guidelines and quality parameters.

THE MOST COMMON PROBLEMS OF ISMS AND THEIR CAUSES

Regarding the use of ISMS, different observations can be made. In some cases, the ISMS is developed in accordance with the applicable standards and laws, and it fulfils its function of information protection. There are cases when the ISMS is partially operational, and cases when it has no relevance to the organization, or it contains irrelevant data, too.

To identify the problems and their causes, the interviews were made with senior and middle management, and the people involved in the implementation and execution of the ISMS. By grouping, the responses received from stakeholders, categories of problems causes were identified. These categories are an inappropriate attitude of senior managers, inadequate development process, short deadline, copying other organisation's regulation, shortcomings in professional knowledge or consultancy.

By the analysis of problems related to structure, content, readability, applicability and compliance to the local and international legislation and the impact of regulations on organisations mainly the following types of shortcomings can be observed:

Problems regarding the ISMS structure:

- Almost all security rules are incorporated in one big regulation.
- All employees have to know and adhere to all security rules and regulations.
- The Information Security Regulation (ISR) contains several rules that are irrelevant to all of the employees.
- There is no role-based, segmentation of the ISMS.
- It is not clear which rules apply to individual employees.

Problems related to the content of the ISMS:

- The ISR contains general methodologies and descriptions instead of referencing them.
- The ISR it too long, up to hundreds of pages, and contains irrelevant information.

Problems related to the readability of ISMS:

- Reading the ISR takes a lot of time, and even if employees read it, they do not remember its content.
- It uses abbreviations and professional terminology, it is incomprehensible to many employees.

Problems regarding applicability of ISMS:

- The ISMS is confused and has overlapping regulations, nobody knows which rule should be applied.
- The ISMS contains contradictory rules.

- If the employees adhere to the ISMS rules, they cannot execute their diyly tasks, which stops the operation.
- The conditions (environmental, technical, economical, etc.) for execution of the ISMS are unavailable.
- The policy and regulation do not fit the operating environment.

Problems regarding compliance:

- Policies and regulations do not adhere to the legal environment.
- The ISMS is a modified version of a relevant laws or standard, but it stays theoretical, it is not integrated into the organisation workflows, it states but does not provide the required protection.

NEED FOR ENFORCEABLE ISMS

As today almost all organisations depend on information availability, confidentiality and integrity, the protection of information is a basic requirement. Failing to implement an operable ISMS is a high risk for organisations.

Analysing the problems shows that the implementation of a poorly designed ISMS, besides failing to protect the information, can cause security risks and hinders the operation of the organisation.

Furthermore, organisations should consider all the factors related to information security which affect operation and prosperity:

- The organisation's own interest in managing confidential information, providing accurate information to partners, customers and employess in order to improve organisation processes,
- Adherance to the legal environment, which enforces not only the compliance on a regulatory level, but the implementation of technical protection measures, too:
  - GDPR compliance cannot be ensured without operational ISMS and technical security measures;
  - The Hungarian Act L. of 2013 and its implementing regulation Ministry of Interior decree 41/2015. (VII. 15.);
  - Implementing information securtiy based on standards:
  - The ISO 27001 certification used to be a market advantage, but by now it has become a requirement;
  - The NIST Special Publication 800-53 helps to implement the technical controls related to information security [11].

CHARACTERISTICS OF ENFORCEABLE ISMS

When analysing ISMS problems, the following categories can be identified: inadequate structure, inadequate content, readability, applicability or compliance. By comparing the inoperable ISMS to the working ones, some characteristics can be observed, which help improve the quality and operability. The following parameter groups show these characteristics.

Compliance with current legislation and standards: this parameter group helps to match the legal requirements and standard's control system with the ISMS. In this category the following characteristics could be identified: building cross-references to the legal requirements, regulations and standards controls and tracking changes of these. Cross-references are needed to legal requirements and standard controls, in a way that helps to audit and verify the compliance. Without having these references it is hard to identify or match the elements of policies necessary to fulfil the external regulatory requirements, which may cause

failure in compliance. Tracking changes of external regulatory requirements generates input for updating the relevant documents of ISMS with reference to the given law and standard version. Usually, this is a process which alerts the stakeholders if relevant laws, regulations or standards are changing which imply policy updates in order to maintain compliance.

Up to date and consistent: these characteristics help to keep the ISMS consistent with business requirements and eliminate overlapping policies. Here the clear definition of policy scope, the documentation map, up to date cross-references and the single definition of terms and rules characteristics were identified. The clear scope and extent of regulations help to keep the ISMS policies consistent. The documentation map defines the scope of each policy and makes the ISMS transparent. The single definition of security rules and requirements makes them defined in only one place and referred from all other documents. The cross-references between documents, help to eliminate the overlaps while help locating related rules and definitions.

Understandable and interpretable: these characteristics make ISMS policies readable and unambiguous. In this category the clear, precise and understandable terminology and language were identified. The language of the policies must be precise, accurate and unambiguous. The security rules must not contain any uncertainty. Terminology and language of ISMS should be understandable by the target audience, even if they are not information security professionals.

Full and complete: these characteristics of the ISMS make the information protection to cover all relevant threats occurring in the organisation during execution of business processes. This means that security rules and requirements of ISMS must cover all relevant threats for the whole organisation, all departments and all employees executing workflows. The security rules and regulations must cover all the workflows of the organisation.

Necessary and sufficient rules: this is one of the most important characteristics group because this mainly influences the operability and the enforceability of the ISMS. The ISMS should provide the necessary protection level, which means the ISMS should have protection measures regarding all information assets ensuring the needed confidentiality, integrity and availability levels. This can be achieved by checking all relevant laws and standards and selecting all relevant requirements for the organisation, then developing and including the corresponding protection rules and measures in the ISMS. The more rules are built into ISMS, the more likely it is that they overlap, so keep minimal, remove unnecessary and merge overlappoing rules. Unnecessary and conflicting rules obstruct employees in executing their daily tasks. No textual parts of laws or standards should be included, they should be referenced instead. No methodology description should be included, they should be referenced, as they are regularly updated.

Hierarchical and role-based structure: the structure of the ISMS should be described in the documentation map to provide an overview of the whole regulation structure, which should be more than the cross-reference between the documents. All policies and regulations in the ISMS should be categorised, in policy, regulation, procedures and supporting documents categories. This helps to separate the diferent execution levels, however there is an interaction between these: the policy level governs the regulation level which drives the workflows producing the supporting documents. The different levels have their role and audience. The policy level contains the strategy and the policies according to which the organisation develops information security. The regulation level states the general security rules to be followed by the concerned departments and employees. The regulation level should be role-based, and the regulations should be available for the concerned departments and employees according to their role in the organisation. The procedure level should consist of

workflows for implementing and maintaining information security. The supporting documents describe setups, authorisation documents, system parameters, test results, maintenance records, incident records, problem records, change records, audit records, system parameters, etc. They are usually the results or the input of the workflows at the procedure level.

Enforceable and executable: to be able to operate the ISMS it is important to train employees, explain the structure and relationship of the policies, regulations, processes and supporting documents. In harmony with the necessary and sufficient rule characteristics these characteristics help minimising the necessary security knowledge of workers in different jobs. General security rules cover knowledge for all employees, must be covered by the Information Security Policy. Department specific rules must be covered by field security policies of the given departments. Activity related security rules must be incorporated into workflows and procedures. To be executable the overall rule system of the ISMS should not contain any conflicting and business process blocking rules. An employee needs to know only those policies, regulations and processes that affect them.

Balances risks and resources: organisations should consider the information security risks, and allocate the necessary resources based on these risks. The ISMS should consider the risks, the possible protection measures and their costs in order to allocate the necessary resources. taking into account the information security risks and resources available to the organization. This means that ISMS must not contain any security rules which imply protection measures that the organisation cannot finance.

CONCLUSIONS

Stevanovic [12] compares two information security standards, and in conclusions shows two essential differences: the implementation cost difference and the main focus of the standards: security and business result achievement. Implementing information security based on ISO 27001 standard in small and medium-sized organisation is not straightforward and needs guidelines [13]. Several inoperable and unenforceable ISMS caused unnecessary costs to the organisations while they left huge security gaps in the system. As external regulatory environment compliance is a must, resources are limited, costs are influenced by the security measures to be implemented, an enforceable risk-based ISMS can be the solution. To achieve this development guideline and quality parameters to improvement enforceability of ISMS were outlined. After implementing ISO/IEC 27001 based ISMS using the guidelines and parameters identified and presented in this article in more than 8 organisations, and getting feedback from them, the gudelines could be improved and the quality parameters could be refined. Therefore, these guidelines and quality parameters are suitable tools for the development of optimised, enforceable and risk-based ISMS. Keeping in mind them and incorporating into the regulation, organisations will be able to improve their ISMS quality and enforceability.

REFERENCES

[1] European Parliament: *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*
Official Journal of the European Union **59**, 1-88, 2016**,**
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN,

[2] Barafort, B.; Humbert, J.P. and Poggi, S.: *Information Security Management and ISO/IEC 15504: the link opportunity between Security and Quality.*
In: 6th International SPICE Conference 2006. Proceedings of the SPICE 2006 Conference, Luxemburg, 2006,

[3] Hungarian Parliament: *Act CXII of 2011 on Information Self-Determination and Freedom of Information.*
Magyar Közlöny **88,** 25449-25482, 2011,
http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/mk11088.pdf,

[4] Hungarian Parliament: *Act L of 2013 on Electronic Security of State and Local Government Bodies.*
Magyar Közlöny **69,** 50241-50255, 2013,
http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/mk13069.pdf,

[5] ISO: *ISO/IEC 27001:2005, Information technology Security techniques - Information security management systems – Requirements*

[6] Chander, M.; Jain, S. and Shankar, R.: *Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach.*
Journal of Modelling in Management **8**(2), 171-189, 2013,
http://dx.doi.org/10.1108/JM2-10-2011-0054,

[7] Gillies, A.: *Improving the quality of information security management systems with ISO27000*.
The TQM Journal **23**(4), 367-376, 2011,
http://dx.doi.org/10.1108/17542731111139455,

[8] Michelberger, P. and Horváth Zs.: *Security aspects of process resource planning*.
Polish Journal of Management Sudies **16**(1), 142-153, 2017,
http://dx.doi.org/10.17512%2Fpjms.2017.16.1.12,

[9] Keszthelyi, A. and Michelberger, P.: *From the IT Authorisation to the Role- and Identity Management.*
In: 4th IEEE International Symposium on Logistics and Industrial Informatics LINDI 2012. IEEE, Smolenice, pp.173-177, 2012,
http://dx.doi.org/10.1109/LINDI.2012.6319483,

[10] Avison, D.E.; Lau, F.; Myers, M.D. and Nielsen, P.A.: *Action Research.*
Communications of the ACM **42(**1), 94-97, 1999,
http://dx.doi.org/10.1145/291469.291479,

[11] NIST: *NIST Special Publication 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations.*
http://dx.doi.org/10.6028/NIST.SP.800-53r4,

[12] Stevanovic, B.: *Maturity Models in Information Security.*
International Journal of Information and Communication Technology Research **1**(2), 44-47, 2011,

[13] Valdevit, T.; Mayer, N. and Barafort, B.*: Tailoring ISO/IEC 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings.*
In: O'Connor, R.V., et al., eds.: *Software Process Improvement.* EuroSPI. Communications in Computer and Information Science **42**, Springer, Berlin & Heidelberg, 2009,
http://dx.doi.org/10.1007/978-3-642-04133-4_17.

Interdisciplinary Description of Complex Systems 17(3-A), 492-496, 2019

LOGGING THE OPERATION AND ENHANCING THE RELIABILITY OF SAFETY-CRITICAL EMBEDDED SYSTEMS USING SELF-TEST

Zsolt Molnár*

Óbuda University, Kálmán Kandó Faculty of Electrical Engineering
Budapest, Hungary

DOI: 10.7906/indecs.17.3.8
Regular article

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

ABSTRACT

There are several solutions to increase the reliability of safety-critical embedded systems (e.g. redundant systems). Where appropriate, achieving the highest possible reliability is always an important goal. The present article also aims to describe a solution for this purpose.

One of these reliability enhancement options – besides redundancy – is the development of a self-testing system that can detect any malfunctions in downtime (during inactivity) or during normal operation. If there is no error, then this self-testing system reports that the system is error-free. The self-testing and event logging system described in this article provides an additional advantage over other solutions. In addition to increased reliability, the root causes of the stored events and information can be discovered and eliminated in case of an error, even, if necessary, by hardware or software changes.

The system outlined in this article – of course – requires further considerations and additions, and the details of circuit and software implementation should be elaborated, but its use in safety-critical systems is clearly beneficial.

KEY WORDS

safety-critical embedded system, self-test, operation and event logging, enhancing reliability, smart city

CLASSIFICATION

ACM: 10010583.10010737.10010744.10010741

JEL: D81

*Corresponding author, η: molnar.zsolt@kvk.uni-obuda.hu; +3616665174;
Becsi u 96/b, Budapest, Hungary, H-1035

SAFETY-CRITICAL SYSTEMS

Embedded systems are systems which include a computer but are not generally used for computing. Safety critical systems are systems whose failure can result in loss of life, significant property damage or damage to the environment [1]. Such systems generally have failure rate requirements ranging from 10^{-5} to 10^{-9} failures per hour or other suitable time period [2], with reliability encompassing the notion that the system is continuously operational and that it is operating with no functional defects during that time. Traditional safety critical domains are the aerospace, medical, chemical processing and nuclear industries. These domains have been conservative, slowly moving to rely upon software systems due to the difficulty of being able to prove that software-based systems will meet their desired operational reliability requirements. Newer non-traditionally safety critical domains including automotive, home automation and civil infrastructure do not always have the experience or the safety culture to help them accurately evaluate the benefits and risks of computer-based controls. Better technologies, processes and standards that improve or ease the use of software in safety critical domains are imperative to protect these domains where cost and functionality concerns may put pressure on safety principles. Regardless of the domain, acceptable mission critical systems are unlikely to be built without good system engineering processes [3].

One of the newest solutions, using a multitude of security-critical embedded systems, is the smart city. There are various elements of smart cities, but the following key areas are typically identifiable:

- smart mobility,
- smart energy,
- smart urban environment,
- smart lifestyle,
- smart governance, city administration,
- smart infocommunication infrastructure common to previous areas, which provides an integrated IT and communication background [4].

Each of the above areas requires numerous embedded system applications that need the use of a safety-critical embedded system. As described above, the presented solution increases reliability and highlights its importance.

ENHANCING RELIABILITY

To achieve the expected reliability of the elements of critical embedded systems (hereinafter referred to as the target units), and to facilitate the post-mortem detection of the events, additional elements are required. So, if the target units contain additional elements outside the security-critical (decision-making) units that implement the following additional activities:

- event and operation logging,
- self-testing (regularly or initiated by external command).

then these elements increase the transparency of the system operation and the resulted safety. The design must be such that, with their normal operation or in case of their failure, these additional elements could not affect the safe operation of the decision-making elements.

Event and Operation Logging

The additional elements collect, store, and make the following information, items, and events available in a suitable form for external request:

- commands, status signals and messages arriving at the target units' information boundary surface in their original (in unencrypted, or possibly in corrupted/damaged) form,
- signals, commands, status signals and messages sent from the target unit as a result of decisions made by the target units, in their realized form and with their parameters (signal level, duration),
- data inputs, configuration activities and other interventions through the controls of the user interface,
- significant changes occurring in power supply and temperature (and other environmental conditions, such as humidity, vibration, etc),
- the activities and decisions of the self-monitoring (self-testing) system,
- events related to event memory units (reading, deleting).

The previously listed events and information must be stored in non-volatile memory units for each event type. Each event has a stored time stamp that indicates the beginning/end of the event with an appropriate (e.g. 1 ms) resolution, with a considered time value for each event. For example, information from a control (on the user interface) or a temperature sensor is unnecessary to sample, to assign time stamps, and to store in every e.g. 10 ms, because the changes at these points are slow. Probably it is sufficient to have intervals of 50 to 100 ms, or even larger, but the event-driven data collection could be used, too.

However, a controlling signal at a microprocessor output, may require storage in the resolution of μs or even denser. It is worthwhile to use a real-time clock (RTC) to create the timestamp, so the absolute and relative time of the events can be determined later, and their timeliness can be examined. If the size of the event-storing memory unit is large enough, it is possible to store the events with the highest density required. When the stored events become obsolete, they can be overwritten, so a circular memory management can be used. The time of data obsolescence should be determined carefully, as an event may affect operation even after a long period of time, therefore, it must be made retrievable much later.

The auxiliary elements allow the reading of the information stored in the event memory units for a unit above the operating hierarchy, and the external (scanner/reader) device connected to it by a special interface. The event of the deletion by command of the event memory unit contents must also be logged, but these events cannot be deleted. Such events should be stored in a separate, protected memory area or memory device.

Self-Test of the Target Unit

The auxiliary elements must be capable of the followings:

- must be able to replace the expected signals, messages, commands, operator interventions at normal operation mode, on the standard boundary surfaces, with predefined test events/signals,
- must be able to register that the decision-making unit responds to test events at what type of events/signals and by how much delay.

The response events/signals for the test events/signals do not get out of the target unit. After checking the functions of the target unit, the results are stored in the memory, and the system returns from the test mode to the normal operation mode. If necessary, an error message is sent to the unit above in the hierarchy.

Self-test can be initiated:

- when powering up the system,
- at regular intervals, provided there is no need for normal operation during the self-test period. The length of the self-test interval (e.g. 1 hour, 1 day) and the suspension of the normal operation mode requires further considerations,

- by the command of the unit above in the operation hierarchy,
- by the operator's intervention.

The identity of the initiator of the self-test, the start and end time, the result of the evaluation and the fact of the possible error result must be stored in a non-volatile memory.

Figure 1 shows the schematic connections between the critical embedded system (also named the target device), and the auxiliary elements for event logging and self-testing. The items presented in Figure 1 include:

- **Target device** blocks (black blocks),
- Signal transmission and signal switching required for normal operation and test mode is performed by **analog and/or digital switches** (rounded gray blocks),
- **Test signal generators** (generate analog and digital signals for self-test) (rounded blocks, some of them are signal converters),
- To the event logging and self-testing unit, the inputs and outputs of the target device are transmitted by **signal converters** (rounded blocks, some of them are test signal generators). Their primary function is level fitting e.g. between different voltage levels, input protection, and, in some cases, galvanic isolation,
- **The event logging and self-monitoring unit controller**, as well as the **associated element**s (memory unit, RTC, environmental sensors) provide the intelligence of the auxiliary elements (gray blocks),

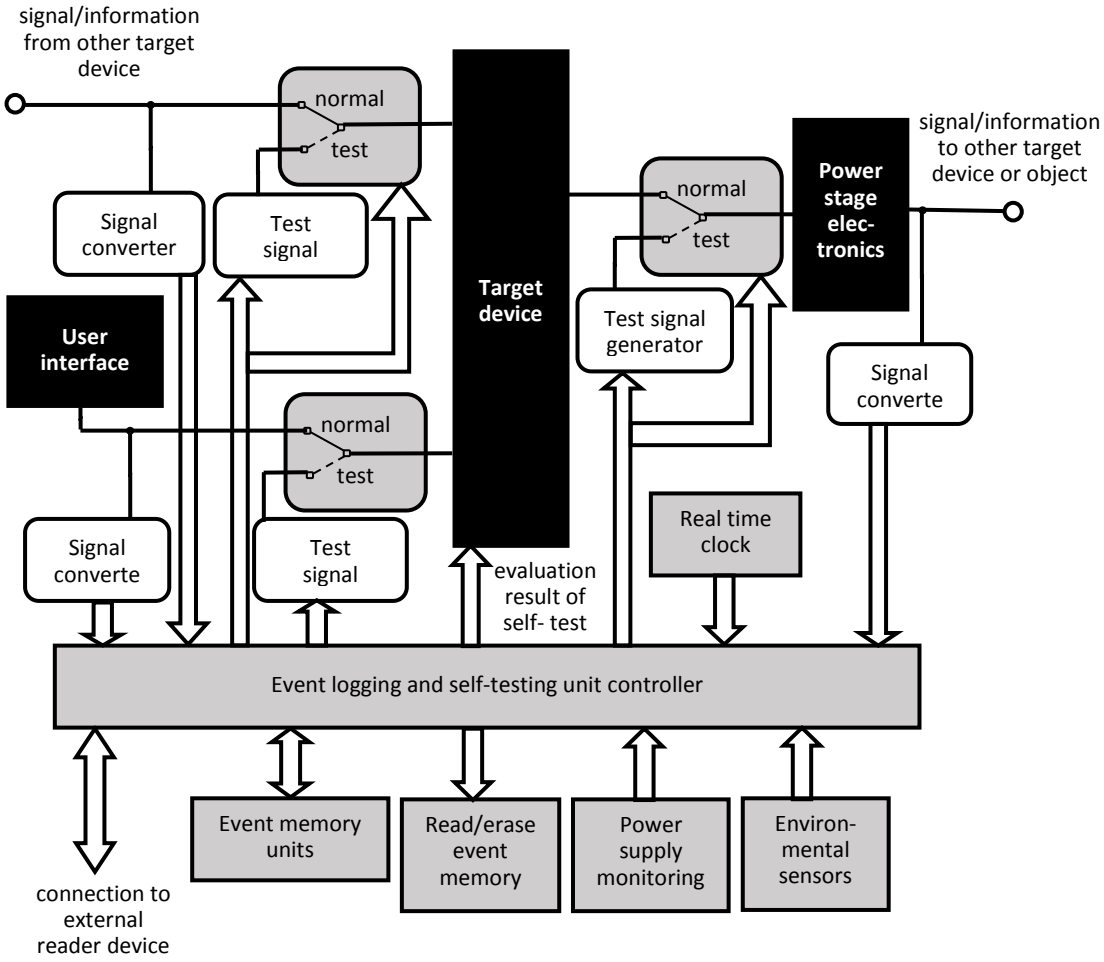

Figure 1. The connections between the target device and the logging and self-testing units.

- Single line connections represent analog/digital signals,
- Arrows represent information flow.

CONCLUSION

For those systems where the stated principle is planned to be applied, the principles of "Design for Testability" (DFT) should be followed. These principles should be considered from system design through the selection of circuit elements and circuit design to the design of the software, as the testability should be planned at system, sub-system and component level [5]. In order to implement the principle described in this article, the boundary scan test method ("digital" boundary scan – IEEE 1149.1 and mixed-signal boundary scan – IEEE 1149.4) can be applied at several points. One of my previous articles described the concept of an integrated circuit to support the self-testing of analogue circuits. [6] Such an integrated circuit is also applicable and can solve many problems during further developments in this field. The solution outlined in the present article can improve the reliability of many safety-critical systems, and it can help to detect the causes of failures [7].

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] Knight, J.: *Safety critical systems: challenges and directions.*
In: Proceedings of the 24th International Conference on Software Engineering. IEEE, Orlando, 2005,
[2] Leveson, N.G.: *Software safety: why, what, and how.*
ACM Computing Surveys **18**(2), 125-163, 1986,
http://dx.doi.org/10.1145/7474.7528,
[3] Kane, A.: *Runtime Monitoring for Safety-Critical Embedded Systems.*
Carnegie Mellon University, Pittsburgh, 2015,
[4] Bakonyi, P., et al.: *Smart City megoldások hat kulcsterületről.*
Budapesti Műszaki és Gazdaságtudományi Egyetem Egyesült Innovációs és Tudásközpont, Budapest, 2016,
[5] Vranken, H.P.E.; Witteman, M.F. and Wuijtswinkel, V.R.C.: *Design for testability in hardware-software systems.*
IEEE Design and Test of Computers **13**(3), 79-87, 1996,
http://dx.doi.org/10.1109/54.536098,
[6] Molnár, Zs.: *Analóg áramkörök beépített öntesztbe vonását támogató integrált áramkör.*
Óbuda University, Budapest, 2009,
[7] Flammini, F.: *Railway Safety, Reliability, and Security: Technologies and Systems Engineering.*
IGI Global, Rome 2012.

Interdisciplinary Description of Complex Systems 17(3-A), 497-502, 2019

THOUGHTS ABOUT THE LIGHTNING PROTECTION OF SOME ELECTRIC VEHICLES

Zoltan Kasza*

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

DOI: 10.7906/indecs.17.3.9
Regular article

Received: 26 December 2018.
Accepted: 31 August 2019.

ABSTRACT

Today, smart devices and technologies, in addition to serving people's individual needs (e.g. smartphones, tablets etc.), are gaining ground in supporting community traffic, healthcare, disaster management as a social public task. As a result of the continuous development of human living communities (villages, towns, settlements), the dominant usage of smart tools and technologies already represents a new quality level (Smart City). Modern logistics support for the public tasks of other settlements or other committed community events takes place through the use of different types of vehicles, in which the use of electric vehicles is also becoming increasingly important. Manufacturers are designing body parts for these vehicles to achieve a smaller weight from various plastic or composite materials in the future, which does not protect the passengers from lightning strikes. From the point of view of life and property protection, the lightning protection of electric vehicles with this technology can be the current area of current research and development.

KEY WORDS

flash hazard, lightning protection, electric vehicles, non-metal framed vehicles

CLASSIFICATION

JEL: L62, O12

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

INTRODUCTION

Nowadays, infocommunication tools and technologies are used by personal users alike, which affects almost every age group of people. In addition to differentiated personal needs, the Internet-based functional support of family and group needs (eg smart heaters, smart homes, smart farms) is simultaneously occurring and becoming more common. Continuous development of network-based digital technologies based on scientific results nowadays allows not only smaller community communities, condominiums to meet community needs, but also the planning and organization of whole villages, towns, and community-based services and services for citizens through the integrated use of infocommunication tools and technologies, and support for implementation. The exact definition of a smart city – SmartCity – is difficult to formulate precisely, but if the former activities are implemented in practice, then we can usually speak of a smart city, with the same public tasks that can be identified and grouped independently of its size. Without the need for completeness, they can be public transport, emergency public tasks, where several different types of vehicles are used. In the course of technological development, different types of electric vehicles are becoming more common on the roads. Manufacturers of bodywork elements of these vehicles are planned to be produced from different plastics and composite materials in order to achieve lighter weight. These vehicles can unexpectedly or planned exit the lightning-protected area during their traffic routes. Nowadays, natural phenomena suggest that global warming caused by human infrastructure activities increases the number of lightning strikes. As much as 1% of temperature rise will increase the number of lightning strikes by 6% per annum [1]. Parameters of strikes are also increasing (e.g. lightning density, peak value). Therefore, in my opinion, lightning protection not only for buildings, but also for these electric vehicles can be a priority research area about smart cities as well.

EFFECTS OF LIGHTNING

The source of damage is considered to be that point where the lightning may strike. In case of vehicles it may be two different points, strike to vehicle (primary effect) and strike near vehicle (secondary effect). Contrary to popular belief, harmful events may not only occur if lightning strikes directly the automobile, but also when it hits next to it. In the latter case the overvoltage induced in the vehicle's electric systems may cause significant damage.

Figure 1. Direct strike to car.

Property damage is caused by lightning strike's inflammatory effect, which builds up the actual economic damage increased by additional costs. Inflammatory and inductive effects may cause further harmful events, so called explosive incidents, the protection against which is managed by the separate field of overvoltage and explosion protection. In case of primary lightning strikes, lightning hits directly the given object. According to one of the insurance companies' data (2016), 90% of the lightning strike damages was caused by secondary effects of lightning [2]. In the technical jargon there is a well-known saying:

„What did not burn was flooded by the firemen."

This saying is true for automobiles possibly bursting into flames. This saying indicates that lightning strike may directly and indirectly cause very severe damages. In order to avoid these harmful effects, automobiles need to be provided with appropriate protection. In case of direct lightning strikes not only the vehicle may be in danger, but also its electric devices and systems (secondary effect). Metal bodywork gives protection against it. In case of indirect (or secondary) effect damage is not done by lightning strike directly, but overvoltage induced by it. It is very difficult to give protection against it.

ELECTRIC AUTOMOBILES TODAY

Automobiles with alternative drives are becoming more and more popular [3]. Their popularity is well represented by the fact that during the Olympic games in Beijing in 2008 and during the 2018 winter Olympics as well, contestants were transported to different locations by a significant number of electric buses [4].

One of the main reasons behind their popularity and spread is the operating costs and the different tax allowances [5]. From the perspective of utilization, these vehicles are quiet and have zero point emission, therefore result in cleaner air, which will be perceived in major cities when they become widespread. Their disadvantage is the range and charging time. Their maximum range is the fraction of their internal combustion engine equivalents and their "refueling" time is longer by orders of magnitude compared to vehicles running on conventional fuel. There is research and already solutions for rapid charging [6], so probably exceptionally long charging time will not be an obstacle to their spread.

It is important to note that for the charging of these automobiles, electricity is coming from the burning of hydrocarbons, so even if they have zero emission locally, on the places of energy production (power plants) they trigger pollution, but to a smaller extent compared to internal combustion engines. An exception is the charging provided with entirely renewable energy.

LIGHTNING PROTECTION OF NON-METAL BODY AUTOMOBILES

Due to the fact that electric cars are being more and more popular, charging stations are expected to be spreaded around countries. This technical field is new so there is no standards for these type of stations, there are only recommendations like VdS 3471 [7] or DKE/AK EMOBILITY.60 [8]. Standard IEC 61851 is about electric vehicle conductive charging systems, parts of it are under development. These recommendations are drawing attention that lightning strike protection is important for electric charging stations. They have some guideline for protecting the stations (Figure 2.) but there are no guideline for direct lightning strike to cars.

In case of direct lightning strike, the lightning current flows through the car body and partly through the suspension, then finally exits through the wheel disk (rim) and is discharged in air towards the ground. The metal body protects the passengers of the vehicle. In order to increase maximum range, manufacturers are planning to produce the bodywork of electric vehicles out

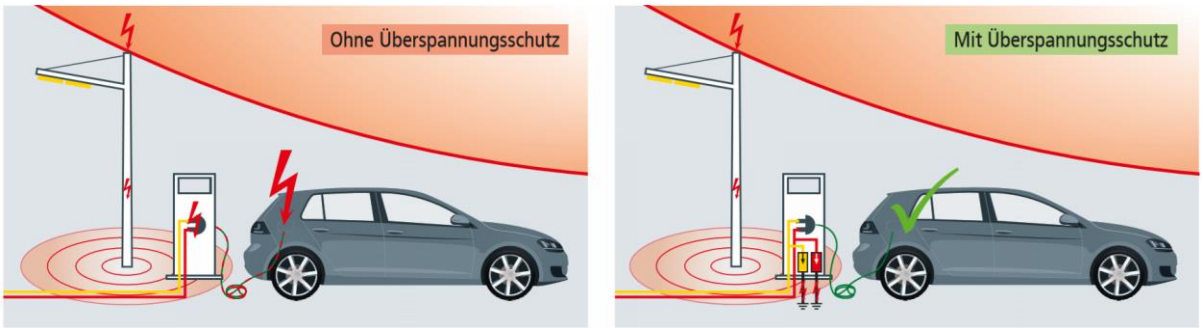

Figure 2. Lightning protection for poles at charging station [9].

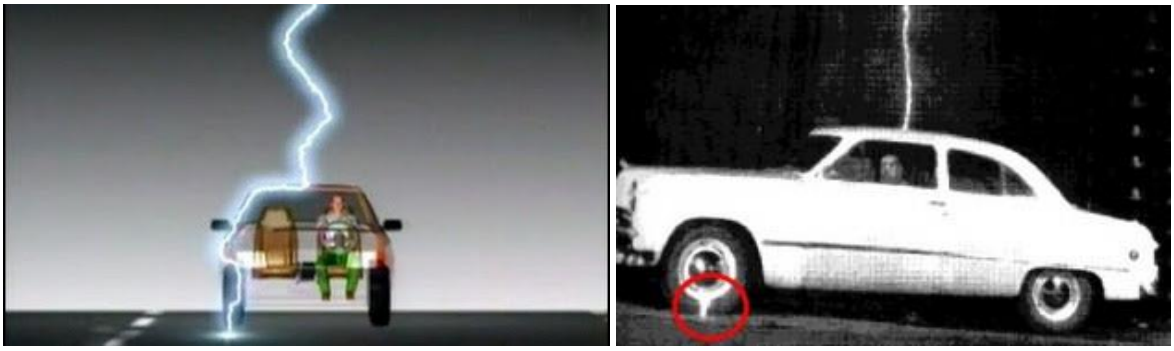

Figure 3. Lightning current route in schematic diagram and in reality.

of non metallic materials (plastics, composite materials). These materials are not conductive, but on the contrary, they have electrically insulating properties. Nowadays, due to the short range, electric vehicles (automobiles, buses) are mostly used in populated areas, and especially in cities.

This gives protection against lightning bolts. Buildings, due to their height, and thanks to lightning arrestors built on them, give safety for the case of lightning strikes.

One might wonder, what happens in case an electric vehicle exits this protected area and what happens in case of s lightning strike? Are passengers in danger? Is there lightning protection?

POSSIBLE SOLUTION

Technically, the aim is to capture the lightning and conduct it towards the ground.

To find the position of the lightning arrestors, we should use the the rolling sphere method. This is a procedure to design the lightning arrestors, according to which the protection is appropriate, if a rolling sphere of given radius can not come in contact from the outside with the protected surface without touching the lightning arrestor. In practice, this means that we are moving a sphere of given radius in the space around the protected object (building, vehicle, etc.) and where the sphere touches an object, that will be the hitpoint of the bolt. With this design method the given object can be protected, because the protected surface will get into the protected space, since the sphere reaches the end point of the protective conductor (better known as lightning arrestor) first. For this design method there are different kinds of 3D software available. As a result, we get a blanket-like surface around the given object, behind which is the protected space (Figure 4).

According to the above mentioned method, lightning is most easily “captured” by a well placed metal body, which therefore is protecting the surfaces. In case of electric vehicles, for

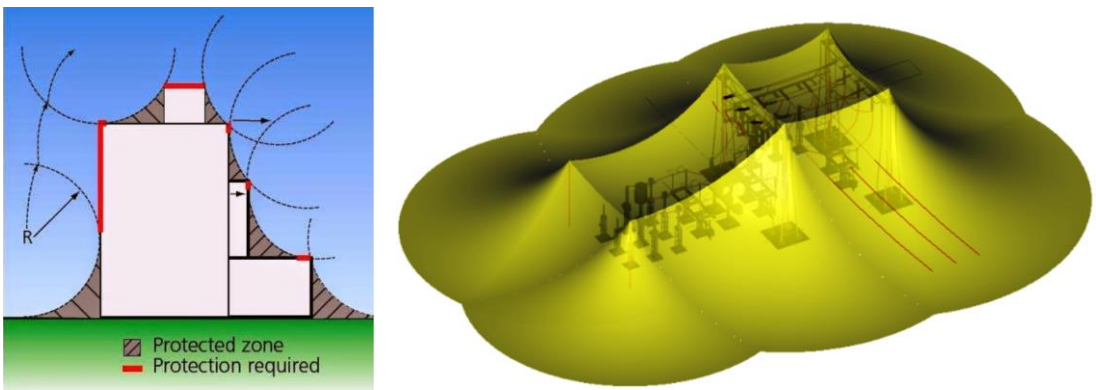

Figure 4. 2D and 3D diagram of the rolling sphere design.

this purpose, a mechanically fixed radio antenna is partially suitable. It is important that the leading wind should not bend the antenna in any direction, since this is protecting a part of the body. For this, adequate mechanical fixing is a must. Moreover, the vehicle must be provided with arrestors on several other points as well.

Figure 5 shows an electric vehicle available on the market, currently manufactured with a metal body. On the left side, the actual, original condition of the vehicle is visible, on the right side the rolling sphere design with the planned arrestors (red markings). We should notice that thanks to the arrestors, the sphere is not contacting the vehicle surfaces, therefore protecting not only the automobile, but the passengers as well. The figure shows one variation of the theoretical design and placement of arrestors. Of course, in case of the vehicle's complete design, the full three dimensional protection of the body should be compiled. For the implementation of lightning protection, not only capturing, but conducting the lightning current is also a problem to solve. When speaking about sizing, the largest stress must be considered, in this case this means a situation when only one arrestor and one conductor would conduct the lightning current. The system should be designed to be capable of conducting even 200 kA of current without damage and warming. For this, a 50 mm^2 cross section conductor is perfect. Lightning current must be conducted to the ground from the body. A solution to this might be a movable conductor that automatically reaches the ground at stops. To avoid excessive and unnecessary requisition (opening of this device at every stop, then closing at start), in practice the movement of this device should be controlled by an electric field strength gauge or by storm warning system. This means that the mobile conductor would be automatically activated when clouds are starting to develop on the sky and therefore the electric field strength measurably changes. A further task is the protection of electric appliances against the induced overvoltage that may appear in such cases. Electric devices in different automobiles are very sensitive to overvoltage. Protection of such appliances can be solved by installing them into metal housings, and electric cables may be threaded through protective tubes or provided with electric shielding.

Figure 5. Rolling sphere design for a commercially available car.

CONCLUSION

Generally I would like to hightlight that the lightning protection of cars and for other vehicles should be designed. This a new area of technical fields and needs a lot of development. The other important technical solution is to pre-create lightning protected routes for vehicles performing public services and make them available for navigation services. It is also advisable to store these data in an integrated database and use it in an interactive way to minimize unintentional passage for the vehicles. To share these data and common experiences (Smart City Connection) in the relationship between smart cities, and to give lectures at conferences or webinars can be also important and useful [10].

REFERENCES

[1] Kulcsár, L.: *Szigetelt villámvédelem (II.).* Elektroinstallateur **2**(5), 34-35, 2012,

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

[3] –: *Alternative-powered vehicles are becoming increasingly popular*. https://www.vg.hu/vallalatok/egyre-nepszerubbek-az-alternativ-hajtasu-jarmuvek-672443, accessed 12nd December 2018,

[4] –: *Self-driving cars and renewable energy: the greenest promising winter Olympics have begun.* https://villanyautosok.hu/2018/02/09/onvezeto-autok-es-megujulo-energia-megkezdodott-legzoldebbnek-igerkezo-teli-olimpia, accessed 11st November 2018,

[5] –: *Tax allowances for electric cars in 2018*. https://villanyautosok.hu/2018/02/02/adokedvezmenyek-elektromos-autora-2018-ban, accessed 14th October 2018,

[6] –: *Electrical Chinese bus charges up in 10 seconds.* https://vs.hu/magazin/osszes/10-masodperc-alatt-tolt-fel-a-kinai-elektromos-busz-0416#!s0, accessed 4th June 2017,

[7] Gesamtverband der Deutschen Versicherungswirtschaft: *Ladestationen für Elektro-straßenfahrzeuge*. Gesamtverband der Deutschen Versicherungswirtschaft, Köln, 2015,

[8] DKE German Commission for Electrical, Electronic & Information Technologies of DIN and VDE: *DKE/AK Emobility.60 Ladeinfrastruktur Elektromobilität,* https://www.dke.de/de/ueber-uns/dke-organisation-auftrag/dke-fachbereiche/dke-gremium?id=3003214&type=dke%7Cgremium, accessed 1st December 2018,

[9] Dehn + Söhne: *Blitzplaner 4. aktualisierte Auflage*. DEHN + SÖHNE GmbH + Co.KG, Neumarkt, 2018,

[10] Martin, A.U.: *The Art and Science of Lightning Protection.* Cambridge University Press, Cambridge, 2008.

Interdisciplinary Description of Complex Systems 17(3-A), 503-510, 2019

THE EFFECTS OF GLOBALIZATION AND CYBER SECURITY ON SMART CITIES

Zsolt Szabó*

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

DOI: 10.7906/indecs.17.3.10
Regular article

Received: 7 December 2018.
Accepted: 31 August 2019.

ABSTRACT

By 2050, 70% of all people will be living in towns and cities. In 1900, it was only 13%. This means that every year, the number of people living in cities increases by seven times the population of New York. Water usage is increasing rapidly too; it has sextupled in the past 100 years; this rate of increase is double the rate of population increase. We must all face the challenge of a large number of people living together efficiently, in an organized way, on Earth, and how they can all access the needed services with the required quality. The term smart city primarily emphasizes sustainability, efficiency, and wide participation in decision-making, infocommunication technology solutions and providing services. The term was coined based on the integration of digital technologies, and the important phenomenon of community development and economic innovation, cities. The main players in the economy of the future are cities. States and local governments alone cannot respond to the challenges of global urbanization and environmental issues. In the development of smart cities, players of the economy and the city dwellers themselves play a more and more important role. The European Union has started programs like this and it is of paramount importance that Hungary actively participates in these, both in central coordination and at the level of settlements. At the same time, it is great help for Hungarian enterprises, too because the products they develop in and for Hungarian towns can be competitive on the international market as well.

KEYWORDS

smart city, cybersecurity, information security, IT security, threats and risks

CLASSIFICATION

JEL: F50, F61, H12, I23, J28

*Corresponding author, η: szabo.zsoltmihaly@phd.uni-obuda.hu; +361 666 5375;
DSSSS, Óbuda University, Bécsi út 96/b., H-1034 Budapest, Hungary

GLOBALIZATION AND INFORMATION SECURITY

Our world suffers three great impacts at the beginning of the 21st century: the population explosion, the increase in life expectancy and the information explosion [1]. The "demographic time bomb" or "population bomb" (the problem of aging) will affect the whole world socially, economically and in other ways. The UN declared 11 July World Population Day in 1989 because the population of the world surpassed 5 billion exactly 2 years before. Since then, world population has increased by more than 2.6 billion, and on 1 July 2018, it surpassed 7.6 billion. World population in 1950 (2.5 billion) has more than tripled by now. Population is still increasing although at a decreasing rate. The United Nations Department of Economic and Social Affairs (DESA) forecasts (assuming medium level fertility) [2] that world population will reach 10 billion by 2055, and by 2100, 11.2 billion people will live on Earth. In 1950, less than 30% of the population lived in cities. In 2018, however, 55% people were city dwellers. The trend is predicted to continue and it is forecasted that in 2050, 68% of people will live in cities. According to the demographic data of the UN (Fig. 1) the population of the world is increasing because the population of developing countries (where many people are very poor) is increasing fast. The population of developed, industrialized countries is decreasing.

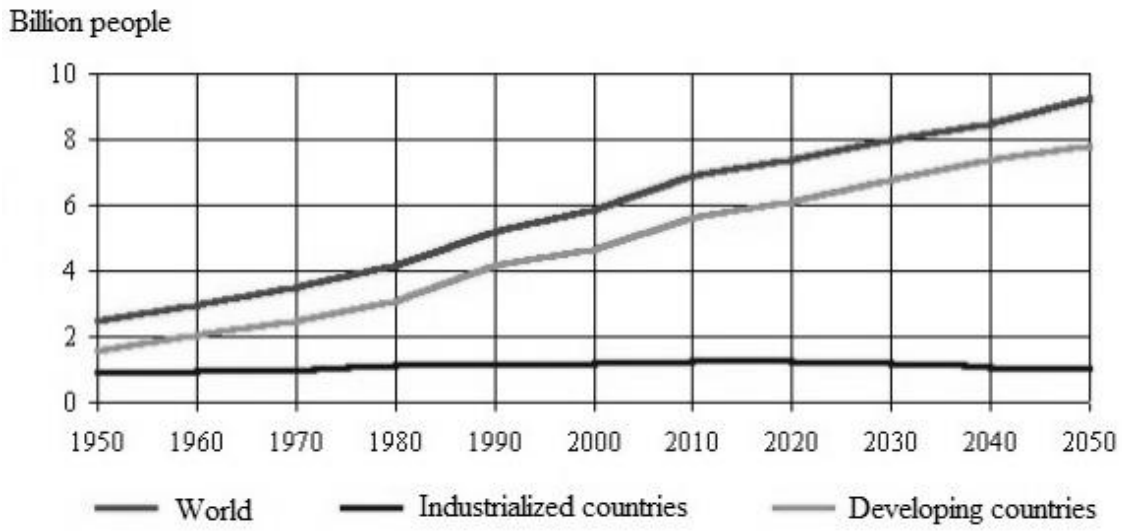

Figure 1. World population between 1950 and 2050.

The UN has been making estimates since 1988 concerning the distribution of the population within countries, and the number of people living in villages, towns and cities. In May 2018, they published the predictions for urbanization until 2050, which was based on the previously mentioned UN population forecast of 2017 [3].

Information concerning the urbanization processes of the world is indispensible for the setting of community development goals both in cities and in the country. The ratio of urban population is considered a basic indicator of economic and social development. For this reason, the increase of urbanization in space and time indicates development well. Urbanization can be charactierized by the increase in the number of cities and the number of people living in the cities. In 1950, less than 30% of people lived in cities. In 2010, the number of people living in cities reached the number of people living in the country. In 2018, 55% of people lived in cities. The number of city dwellers in the world has increased 5,6 times (to 4,2 billion) since 1950 (751 million), while the number of people living in the country has only doubled since 1950 (to 3.4 billion) (Fig. 2). This tendency is forecasted to continue—in 2050, 68% of people will live in cities [3].

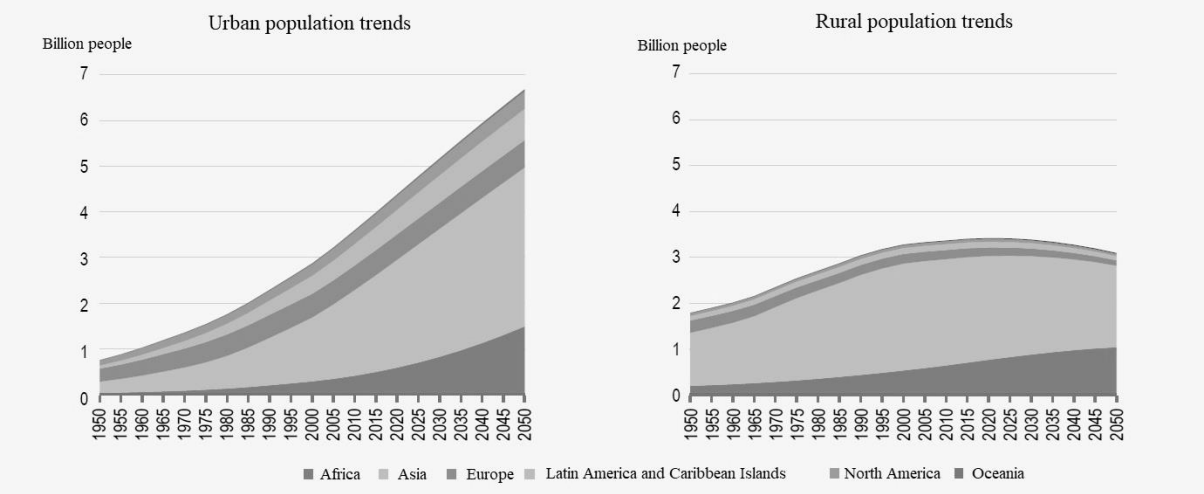

Figure 2. Population in cities and in the country between 1950 and 2050.

Forecasts show that urbanization and the general increase in world population will result in the number of city dwellers increasing by 2,5 billion by 2050. Nearly 90% of this will concentrate in Asia and Africa. It can be seen that by 2050, nearly 70% of people will live in cities. Urbanization is a dual process; on the one hand it means the increase in the number of cities, while on the other hand it means the expansion of urban functions, the development of infrastructure and city lifestyle.

One of the main tools and also channels of globalization since the 1990s is the explosive development of the Internet and mobile telecommunication technologies. As computers developed, after a time, the Internet was created [4, 5].

Web 1.0 covers the period between 1989 and 2004-2005. It is also referred to as the era of information connections. In other words, this was called “read-only web” [6]. In the early days of the Internet, you could search for and read information on the Internet. Very little interaction was offered to users, connection to websites was nearly impossible, and content production was practically non-existent. Website operators did not want to communicate with the visitors of the website, just provide them with information, anybody, any time. Therefore, at the dawn of the Internet, it was very static, “read-only”, and with very little content produced. Each website had a limited number of people responsible for it. The websites could not be edited by anyone, just people who had permission to do it and access. It was their responsibility to keep the site up-to-date and to transmit the fresh content to the users.

The second generation of the Internet, Web 2.0, defined as “readable and writable web” [6]. Over the years it had very many definitions. Web 2.0 is a revolution in the commercial world of the IT industry, used as a platform. The basic difference between Web 1.0 and Web 2.0 is that there were few content producers with the first generation. Most Internet users behaved like people in a shop. They browsed the selection but did not add anything to it. On the other hand, in the era of Web 2.0, anybody can be both a seller and a buyer at the same time. Many technological solutions have been created to help users create their own content, and thus facilitate the mass production of content.

Web 2.0 is an umbrella term, including a multitude of Internet services. All such services are based on the power of the community. Users create content together or share each other’s information [7]. The democratic nature of Web 2.0 is shown by a large number of Niche groups (closed communities of friends), who can exchange, label, comment or link an content, be it text, sound, images or video, to sites within or outside the group. Web 2.0 was the basis of the first social media sites, too. It is hard to imagine the world, when social media

sites were not part of our everyday lives. By now, the Internet has become a utility. Not a day passes by when we do not look up on the Internet what has happened in the world. We no longer get the most news from newspapers, the radio or television, but read news on the Internet or listen to it on net radio. Today's households require service providers to develop; this can be seen in every service sector. Whatever we plan to buy, we first look it up on the Internet, read about its properties and read opinions and other people's experiences and only then decide to buy it. We select the best or cheapest shop on the Internet and buy the product or service there.

As opposed to Web 1.0 and Web 2.0, Web 3.0 is no longer made for people only, and not only people will use it. Nowadays the Internet can be accessed from nearly everywhere in the world [7]. Now global IP traffic has exceeded one zettabyte (10^{21} byte). Only in Google, 3 600 000 searches are executed every minute, and in one year, four billion people will have Internet access. Facebook had more than 2 billion active users in 2017. Web 3.0 is an exceedingly tailored web, which is decentralized and provides users with more possibilities than ever before. As a result of the population explosion and information explosion, we must all face the challenges of the global digital world; the most important challenge is how all these people can live together efficiently, in an organized way, and how they can access the right type of digital and other services in the right quality and with the required security. Another challenge is to train enough specialists who can design, install and operate the necessary systems.

CYBERSECURITY ISSUES IN A SMART CITY

Currently there is no universally accepted definition for cyberspace. The term Cyberspace (cybernetics + space) was coined by William Gibson science fiction writer in 1982. It first appeared in his short story "Burning Chrome" [8], then in his 1984 novel Neuromancer [9]. Over the years there have been countless definitions for cyberspace [10, 11]. Based on these, in general, cyberscpace can be considered a system of electronic communication devices and systems (computer networks, telephone lines, satellite systems etc.) and the virtual space composed of the services provided on these. As the Internet is growing and spreading, more and more formerly independent communication networks, systems, devices and services are connected to it, or simply being replaced by the Internet. Therefore, it is not surprising that in everyday use, the concept of cyberspace is more and more understood as the Internet itself, or the virtual world accessible through the Internet. The technological revolution mentioned earlier and cyberspace are changing our everyday environment more and more intensively, from communication, through access to services, to the data available to decision makers.

The term "Smart City" was invented in the USA. A city can be called smart if it achieves sustainable economic development with balanced investment in traditional and digital infrastructure, and human and social capital, with the active participation of the community, in an environmentally conscious way [12].

For a city, being a smart city is a process; it involves continuous development. Intelligent cities consist of many different and connected components, which continuously exchange data. Components can be intelligent networks, building automation systems, intelligent vehicles (driverless or pilotless vehicles, and others), Intenet of Things (IoT) sensors and using the cloud platform [13].

CYBERATTACKS AND THREATS

Smart cities process an enormous amount of data, due to the smart devices. These devices collect and generate many different kinds of information (sensor data, location data, common routes, and even customs of the citizens). Processed properly, these data provide valuable

information in many areas [14, 15]. Internet-enabled devices, for example, can diagnose themselves, and so the can predict maintenance needs or even future breakdowns. Examining user customs can also help manufacturers to develop more convenient and safer devices. Another possibility is that manufacturers can pass on or sell aggregated anonymous data to other organizations, this way helping design and maintenance. This, however, is both a possibility and a danger (Figure 3) [16, 17].

Smart cities are comprised of a highly complex, interdependent network of devices, systems, platforms, and users. Smart energy, utilities, water and wastage, parking and automotive, industrial and manufacturing, building automation, e-government and telemedicine, surveillance and public safety are just some of the verticals that vendors and governments must secure. Urban population is on the rise worldwide and smart city development projects are

Figure 3. The challenge of securing smart cities: cyberattacks and threats.

are harnessing the power of the Internet of Things (IoT) to develop more intelligent, efficient, and sustainable solutions [18]. However, digital security investments in smart cities are severely lagging thus seeding the future vulnerabilities of the IoT ecosystem. Cyber attacks targeting IoT devices are rapidly increasing, as more people and organizations deploy them. IoT devices that are connected to the Internet but do not have a password set, or are often operated with the initial settings, are likely candidates to be targeted next. The security measures covering IoT devices are urgently needed [19].

IoT devices, which have smart functions and are connected to the Internet are among the most important and fastest growing segment of technology. The value of IoT is estimated to reach 83 billion dollars by 2022. The security of all the data used by IoT is a serious challenge. According to recent statistics, attacks against the IoT have increased sixfold between 2014 and 2018. These incidents affect all players of the sector, from manufacturers and their suppliers to operators. manufacturers have to protect more and more data. A device connected to the Internet may process several Gigabytes of data in a single hour. In the third quarter of 2018, only in the USA, on the telecommunications network of AT&T, 24 million connected devices communicated with each other. If these data are stolen or made public, it can lead to serious damage, and hefty fines in this better and better regulated environment. IT experts therefore have to guarantee not only the fast and efficient use of data but also their secure handling, according to GDPR [20] and other laws and regulations. Experts say that an obvious solution of protecting sensitive data is removing the sensitive parts from data before they enter analytical platforms. One method to do this is data masking, which involve changing sensitive data to random characters. Its advantage is that the format of the data remains and therefore the data can be used in various analyses and statistics.

CYBER PROTECTION AND CYBER STRATEGIES

As infocommunication devices and services develop rapidly, more and more cyberattacks are directed towards the state, civilian and private sector [21, 22]. In the past few years, several international organizations have offered recommendations, strategies and norm frameworks so that states and social and economic players can develop their own cyber protection structure and generate the minimum requirements that are essential safe and secure existence in cyberspace. The NATO cyber protection centre (2010) [23]; the International Telecommunication Union of the UN (2017, 2018) [22, 23], the European Union Agency for Network and Information Security (ENISA) (2017, 2018) [26, 27], Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [28]. These all call our attention to basic and interconnecting security situations:

- any member of information and communication networks – whether international, state or civilian – can be a potential victim of cyberattacks,
- cyberattacks can have serious national security and economic consequences, and can endanger the everyday life of a society,
- defence agains threats is a task at the international, national and individual user level as well.

CONCLUSION

At the beginning of the 21st century world economy was far more integrated than in the middle of the 20th century. It is visible that there are three large centres in world economy: North America, Western Europe and Eastern Asia. China is the most populous country in the world and the largest aging society. The problem of aging societies affect the whole world in one way or another. The main factors of economy in the future will be cities. “Smart city” is not a state, rather a process, the result of continuous development. The smart city concept,

however, is a serious security risk all over the world, due to the infocommunication and other systems, which are not always secure. The first – and perhaps most serious – security issue is dependence. Dependence on infocommunication systems and the services they provide. When smart services falter in a city space, which is overcrowded in itself, and whose efficient operation heavily relies on information systems, enormous chaos ensues. From transport through logistics to public utilities, all systems are more and more interdependent. In this situation, a carefully planned and executed IT or information attack can easily bring a city to its knees. There will be no disposal of waste, passanger transport falters, there is no transport of goods, no communication; there is not even news about what happened. Of course, this is only fiction now, and smart cities have no alternative. Therefore security and secure systems are the only alternative for the future.

REFERENCES

[1] Iván, L.: *Physiological and social phenomena of aging. Current issues of aging.* Journal of the Hungarian Academy of Sciences **2002**(4), 412-418, 2002,

[2] United Nations (DESA): *The 2017 Revision of World Urbanization Prospects.* https://esa.un.org/unpd/wup, accessed 13th May 2019,

[3] United Nations (DESA): *The 2018 Revision of World Urbanization Prospects*. https://esa.un.org/unpd/wup, accessed 14thMay 2019,

[4] *Internet History of 1990s.* https://www.computerhistory.org/internethistory/1990s, accessed 15th May 2019,

[5] –: "*World Wide Web Timeline"*. Pews Research Center,

[6] Viswanathan, G.; Mathur, D.P. and Pradeep, Y.: *From Web 1.0 to Web 2.0 and beyond: Reviewing usability heuristic criteria taking music sites as case studies*. https://www.academia.edu/8381037/From_Web_1.0_to_Web_2.0_and_beyond_Reviewing_usability_heuristic_criteria_taking_music_sites_as_case_studies, accessed 18th May 2019,

[7] Cohen, B.: *Urban Mobility: Web 2.0 (Uber) vs. Web 3.0 (IoMob)*. https://medium.com/iomob/urban-mobility-web-2-0-uber-vs-web-3-0-iomob-2e424a99f8bd, accessed 20th May 2019,

[8] Gibson, W.: *Burning Chrome. Burning Chrome.* HarperCollins Publishers Inc., New York, 1986,

[9] Gibson, W.: *Neuromancer*. 20th Anniversary Edition. Ace Books, New York, 2004,

[10] Haig, Zs.: *Information, Society, Security*. NKE Service Ltd., Budapest, 2015,

[11] Gémes, Cs.: T*he cyberspace and its actors.* Hadmérnök **13**(3), 403-415, 2018,

[12] Giffinger, R.: *Smart cities Ranking of European medium-sized cities.* http://www.smart-cities.eu/download/smart_cities_final_report.pdf, accessed 23rd May 2019,

[13] Tokody, D.; Albini, A.; Ady, L.; Rajnai, Z. and Pongrácz, F.: *Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city*. Interdisciplinary Description of Complex Systems **16**(3-A), 384-396, 2018, http://dx.doi.org/10.7906/indecs.16.3.11,

[14] Szabó, Zs.*: Cybersecurity issues of pension payments.* In: IEEE 15th International Symposium on Intelligent Systems and Informatics. IEEE, Subotica, 2017, http://dx.doi.org/10.1109/SISY.2017.8080569,

[15] Szabó, Zs.: *Cybersecurity issues in industrial control systems.* In: IEEE 16th International Symposium on Intelligent Systems and Informatics. IEEE, Subotica, 2018,

[16] Swati, K.: *TheHackerNews: Baltimore City Shuts Down Most of Its Servers After Ransomware Attack.*
https://thehackernews.com/2019/05/baltimore-ransomware-cyberattack.html, accessed 25th May 2019,
[17] Gibbs, S.: *Ransomware attack on San Francisco public transit gives everyone a free ride.*
https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware, accessed 26th May 2019,
[18] Help Net Security: *Cybersecurity challenges for smart cities: Key issues and top threats.*
https://www.helpnetsecurity.com/2019/08/21/cybersecurity-smart-cities, accessed 21st August 2019,
[19] Abdulmalik, H.; Jingqiang, L.; Fengjun L. and Bo, L.: *Cyber-Physical Systems Security – A Survey.*
IEEE Internet of Things Journal **4(**6), 1802-1831, 2017,
http://dx.doi.org/10.1109/JIOT.2017.2703172,
[20] –: *Regulation (eu) 2016/679 of the european parliament and of the council.*
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, accessed 26th May 2019,
[21] Pető, R.: *Security of smart city.*
Interdisciplinary Description of Complex Systems **17**(1-A), 13-19, 2019,
http://dx.doi.org/10.7906/indecs.17.1.3,
[22] Kiss, M. and Muha, L.: T*he cybersecurity capability aspects of smart government and industry 4.0 programmes*.
Interdisciplinary Description of Complex Systems **16**(3-A), 313-319, 2018,
http://dx.doi.org/10.7906/indecs.16.3.2,
[23] NATO (2010): *Strategic Concept adopted by the Heads of State and Government of NATO member states in Lisbon for the protection and security of member states of the North Atlantic Treaty Organization. Active involvement, modern protection.*
https://2010-2014.kormany.hu/download/b/52/20000/nato_strategiai_koncepcio.pdf, accessed 27th May 2019,
[24] ITU (2017): *Definition of Cybersecurity.*
www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx, accessed 27th May 2019,
[25] ITU (2018): *Global Cybersecurity Agenda (GCA).*
www.itu.int/en/action/cybersecurity/Pages/gca.aspx, accessed 29th May 2019.
[26] ENISA (2017): *Cyber Europe.*
www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme, accessed 28th May 2019,
[27] ENISA (2018): *National/governmental CERTs Baseline Capabilities.*
www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/baseline-capabilities, accessed 30th May 2019,
[28] –: D*irective (eu) 2016/1148 of the european parliament and of the council.*
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN, accessed 5th June 2019.

Interdisciplinary Description of Complex Systems 17(3-A), 511-519, 2019

THEORETICAL STUDY OF CLOUD TECHNOLOGIES

Attila Albini*, Dániel Tokody and Zoltán Rajnai

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

DOI: 10.7906/indecs.17.3.11
Regular article

Received: 8 December 2018.
Accepted: 11 September 2019.

ABSTRACT

One of the main objectives of the smart city is to improve the quality of life. The information and communication technology (ICT) components are used as vital parts of the system. Increasing efficiency is the base of the smart city's sustainability. Therefore to increase the efficiency of ICT is crucial. Although cloud technology is just one possible building block of the ICT infrastructure its theoretical study used by the smart city is important because the cloud building technologies can be extended to the use of other ICT technologies. Because of these possibilities, one should study the potential regularities of cloud operation which affects among other things, the availability, capacity, flexibility and scalability topics as well.

KEY WORDS

cloud, definition, requirement, building, technology

CLASSIFICATION

ACM: C.0, H.1.0, K.6.4

JEL: D85

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

INTRODUCTION

The cloud technology in information and communication technology (ICT) is a young and cutting-edge area. This is due to the fact that from the individual mobile to a full realization of virtual data centers it is possible to provide service over the network. Many people do not know that their communication device uses such a service. Users do not use these facilities consciously.

Most people who have heard about cloud think of clouds provided by the telecommunications and information technology service providers. Although anyone can use these services nowadays, the first clouds were used at companies in a closed way. These were private systems with unique implementation. Over time development enabled the standard usage and economic services could appear. Later the advance of technology has provided some management solutions that allowed the measurability of this technology. This enabled the cloud as a service to external partners. Today the conscious use of clouds affects the flow of information. Thus, cloud usage indirectly affects also the rankings in the academic sphere [1, 2].

Documents that are found on topic [3] of cloud computing do not provide sufficient insight into the technologies used for cloud construction. These technologies themselves are used separately and solutions of manufacturers are well documented. The synthesis of implementations and a combination of technologies, namely technologies of cloud building are less documented. This study will cover the definitions, requirements and the main building technologies of the cloud. These technologies are based on the recommendations of the principal component-manufacturers.

DEFINITIONS

The internationally agreed definition of cloud by the National Institute of Standards and Technology (NIST) is based on the cloud's requirements. The organization provides only an indirect definition and this definition does not include the goal of the cloud. The system without a goal looks like a system that only exists for its own sake. Therefore the definition should be made more applicable which contains the goal to be achieved.

The cloud service has three actors: the customer, the vendor, and the legislator. Because of this, the definition is possible from more aspects. The purpose of the user who is the official customer of the service is other than the purpose of the vendor who is the manufacturer of the technology. Furthermore, the legislator has independent control. The different interests of the actors justify the conclusion of a service contract in which the parties should jointly formulate what they mean for services.

The proliferation of cloud systems and the increasing number of disputes that are likely to appear require the definition of formal cloud service. Legislators can use this definition to statutory interpretation and dispute settlement. Furthermore, the robust cloud service providers are multinational companies nowadays who have taken into account disaster tolerance issues and have formed their systems in several countries or continents. So harmonization and internationally accepted interpretation are needed.

Definition of the cloud is possible from the following aspects:

- independent,
- user,
- contractual,
- technological.

INDEPENDENT ASPECT

From an independent perspective, the cloud definition, identification and classification types by NIST mentioned above can be the base in the legal systems of individual nations and the international alignment. According to this definition "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [4].

This definition seems wordy and not exactly defined. This applies in general to an independent approach. The aspects of these definition types are to describe the behavior of the system and the system is determined by its behavior. From a special aspect, by contrast, the definition can have a more closed shape.

USER ASPECT

From the user approach, the cloud can be defined as such: the cloud is a combination of flexible computing services that can take over the interface of the service provider in order to implement more cost-effective business processes.

The economic interests of the customer are dominant at this definition. The goal is the long-term cost-effectiveness [5]. It does not need a large IT operation to be maintained in case of recourse cloud services as a customer uses their infrastructure. Furthermore, the introduction of individual systems can be more flexible to manage.

CONTRACTUAL ASPECT

From the aspect of the customer and supplier cloud can be defined as the following: the cloud is a flexible information and communication technology service system that is made possible through an interface specified in the contract and agreed by both parties in quantity and quality.

This definition is based on the parameters specified in the contract. This contract is an interface interpretation which is served between the supplier and the customer.

TECHNOLOGICAL ASPECT

From the topic relevant technological aspect, the cloud can be defined as the cloud is a flexible and measurable information and communication technology system in which the services behind the interface are as far as possible independent of the faults and limitations of physical and logical devices.

This definition is based on the technology. Intrinsic properties of the cloud appear here which arise from the technologies used for building [5]. Before the introduction of technologies in order to increase transparency, one should discuss some of the basic concepts and requirements.

REQUIREMENTS

The analysis of cloud building technologies shows that the most important characteristics of the cloud include reliability, component variability, flexibility and the measurability of the services. The technical requirements of the components can be grouped according to the following topics:

- availability (existence),
- virtualization of necessary resources (structural and energy knowledge),
- virtualization of implemented services (validation),
- flexibility (control and change management).

AVAILABILITY

The cloud is always possible to operate because business-critical subsystems can be realized in it. The increase of the system's reliability can be achieved using a reproduction of physical and logical components. It is also known as redundancy. One of the features of reliability is availability [6, 7]. This is a percentage to the scanned object which is the working percentage of the time interval in question.

Generally, automation has to be introduced in the system management layer up above 90% planned availability. The finances spent on the degree of automation are growing rapidly to increase designed availability. The curve's asymptote is at 100% planned availability. This is analogous that 100% safety could be achieved neither with risk assessment nor with risk reduction.

The level of availability assumed by the service provider is often recorded in the contract. A value above 95% is called high availability (HA) [5]. The big cloud providers take "fiveniner" uptime, which is 99,999%.

RESOURCE VIRTUALIZATION

The cloud works to the extent possible regardless of the individual resources. Its availability and capacity are higher than the individual processing units' ones [8]. The used cloud building technologies make this property possible, among which virtualization is highlighted. This means that the virtualized architecture layer's real resources are covered, and only the required quantity and quality capacity are presented to the higher layer in a necessary way.

This technology enables the services' measurability, too.

SERVICE VIRTUALIZATION

The implementation of cloud services must be measurable. An implementation of service may affect several devices and several components of services may be present on one device. Because of this, the concept of virtual service was introduced.

The service to be detected is displayed as such. The relevant system components' relationships are modeled for compiling virtual services and these components' dedicated availability and capacity data are used to measure the service being provided [9]. These metrics are usually included in the contracts.

The use of virtual services is essential to establish the appropriate cloud management layer.

FLEXIBILITY

The system components which implement cloud services have to be flexibly parameterized. The virtualization has to be implemented in such a way that the presentation of resources can be properly granulated. The additional requirement is that dedicated capacity can be flexibly assigned to the services. If the operating processes permit these system parameters can be changed on the fly [10]. Adequate performance of individual subsystems can easily be formed, thereby enabling cost-effective operation.

BUILDING TECHNOLOGIES

Several manufacturers' realization came to light about the previously mentioned increase in availability. Considering the principle of operation it can be grouped around a few core technologies.

Each technology is based on redundancy registered in the system. The strongest method is the complete duplication of the components (2*n* redundancy). The simplest case means that one

more than necessary components are deployed in the system (n + 1 redundancy). Passive and active operation modes are possible in both cases [5].

In a passive operational mode, only one component serves the users and another component takes over the role of a faulty component. In an active mode, all the components serve the users and the faulty component's load will be transferred to other elements.

Most outlined building technologies below can be found in all the architectural layers of the cloud. For many, some technologies are more or less familiar. However, they are not always aware of its logical system and the manifestation of these technologies in the cloud layers.

The core technologies:

- cluster Technology,
- grid technology,
- virtualization,
- split technology.

CLUSTER TECHNOLOGY

Clustering means that more components can perform the same activity but it seems a single service looking from outside. The primary goal is to increase availability.

This building technology has democratic governance. This means that the cluster elements maintain an equal relationship with each other. In case of failure the components still being used jointly decide on the inner constellation to continue providing the service. This democratic governance has the condition that a very fast communication channel has to be established between the members. This channel can be a shared channel or device [11, 12]. Figure 1 shows the working schema of the cluster.

The clusters can be passive (fail-over). In this case, if one member implements the feature and an error occurs, another member will continue. The cluster can be active (load-balance) when each member is involved in implementing and in case of failure the load of the failed member takes over [12].

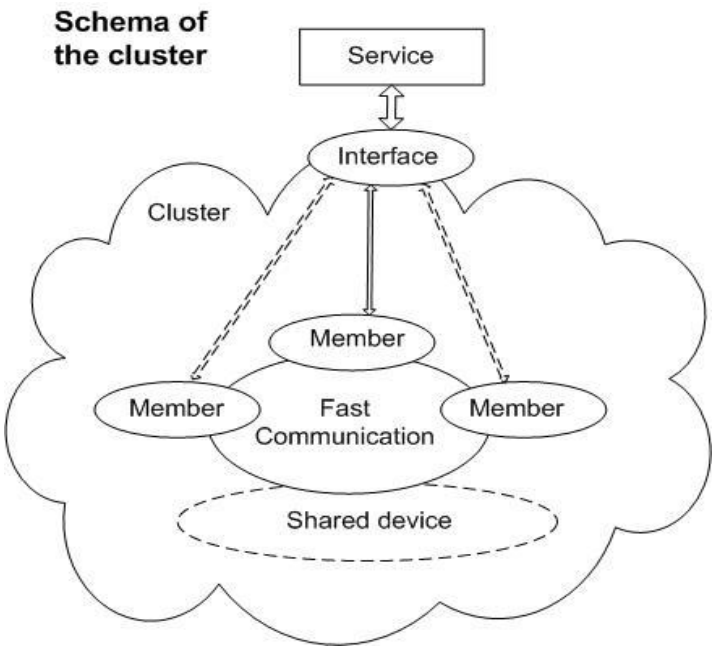

Figure 1. Working schema of the cluster.

Advantage:

- fast communication between members due to rapid fault management.

Disadvantages:

- disadvantage stems from the need for fast communication because long distance could not be between members,
- because of the predictability of charges cluster should be implemented by physical devices with the same parameters.

GRID TECHNOLOGY

The Grid technology means that more components perform the same activity but looking from outside it seems a single service. The primary goal is to reduce the processing time.

In contrast to the cluster, it has autocratic governance. A controller component controls the operation of the grid and manages its internal administration, directs the faulty member's failover, performs the presentation of services. The most important task is to divide the operations between members related to its capacitive possibilities [13]. The grid does not need fast communication between the members. Figure 2 shows the working schema of the grid.

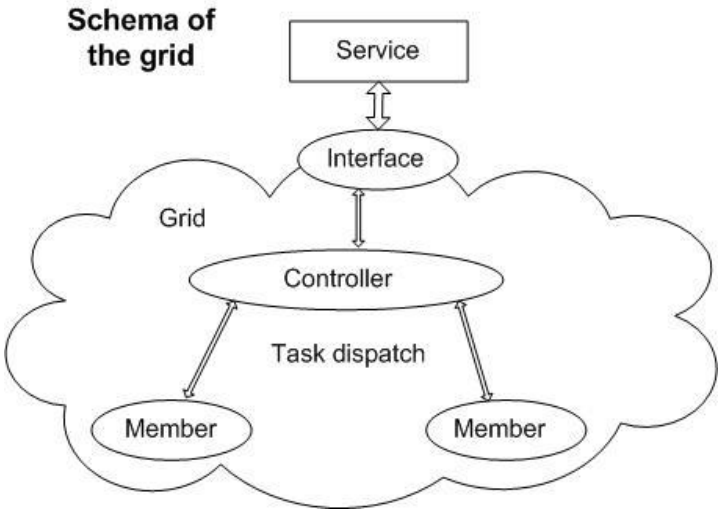

Figure 2. Working schema of the grid.

Due to the operating principle of the grid, it always works in active mode (load balance). If the controller continuously administers the capacity and processing capability of the members, the use of a variety of infrastructure is accessible. In the absence of administration, however, only the same building blocks could be used for building the same instruments.

Advantages:

- the grid can be built on a large distance,
- building blocks with different parameters may also be utilized.

Disadvantage:

- due to the task-oriented working method, it has very slow error handling.

VIRTUALIZATION

As previously mentioned the virtualized architecture layer covers the real resources and presents only the required quantity and quality of capacity to the higher layer in a necessary way. This technology made possible the further development of cluster and grid technologies and cloud formation [14]. Figure 3 shows the virtualization's schema.

The virtualization first appeared on servers as a new layer under the layer of the operating system. Later this technology appeared in the network topology, in the storage's data allocation layer, then in the cloud management layer. It is now up to the entire data storage layer, to the entire server layer, to the total manifestation of network with minimal exceptions and the system management layer.

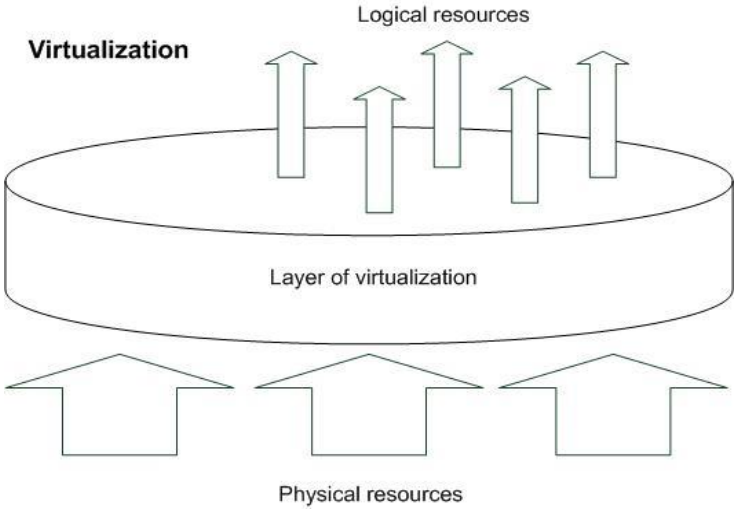

Figure 3. Method of the virtualization.

SPLIT TECHNOLOGY

The emergence of large data centers and thus increasing availability intention formulated new needs. The risks associated with the site becoming unusable must be reduced to a minimum. This demand continued to grow with the appearance of clouds.

Many manufacturers have developed solutions but the principle is similar. The basic element of the implementation is a splitter component which typically works in the low level data storage layer of the architecture. This feature controls the communication traffic of the higher layers and directs it to multiple directions. This method enables data replication to other sites [15]. Figure 4 shows the split technology.

The replication can be synchronous, asynchronous or dynamical. In the synchronous method, the system waits for the write-through of the other side's data. In the asynchronous method, there is no waiting only a communication journal is used for following the primary site. In the dynamic method, the result of waiting depends on the actual performance.

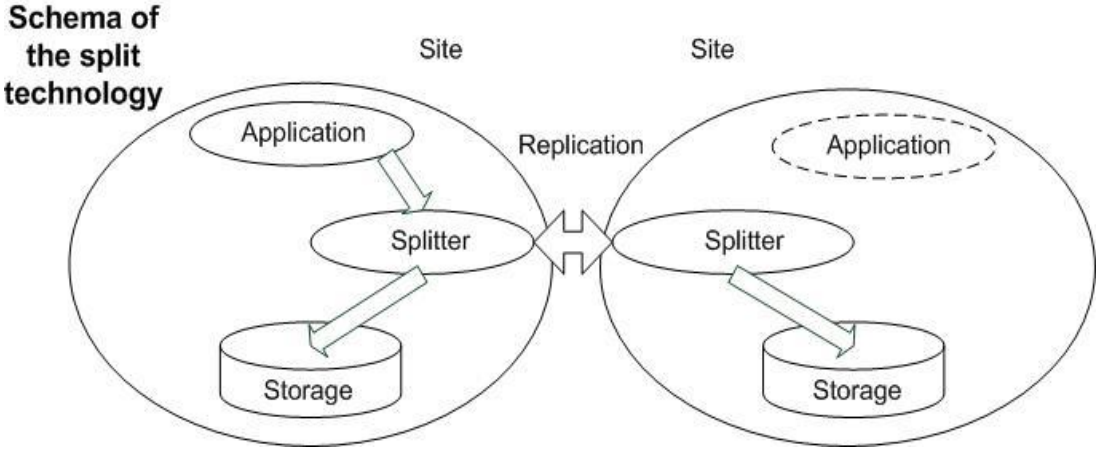

Figure 4. Working schema of the split technology.

If a site fails then another site executes the components of the system. Furthermore, the sites could be the disaster site of each other. The manufacturer's platform and the implementation are carried out within the expected influence on the switching time (from a few minutes to a few hours) and cost requirements of the solution as well.

Nowadays there are new solutions where the splitter component is situated in the virtual layer. The storage layer is controlled from this layer through a logged communication channel.

CONCLUSIONS

The cloud can be approached from multiple aspects. Independent, user, contractual and technological angles can be tested in the definition. The independent definition includes the system's behavior. The user definition includes cost-effectiveness. The contractual aspect specifies the parameters of the system. The wording from the technological aspect implies that the most important requirements are availability, independence, flexibility, and service orientation.

The cluster, grid, virtualization and split technologies enabled to satisfy the discussed requirements of the cloud. The cluster is used to increase availability. The Grid is used for faster processing time. Virtualization is used to carry out flexibility. Split technology is used to implement disaster tolerance.

These technologies are in use today in all architectural layers of the cloud. The technologies are not pure but mixed and complementing each other. Furthermore, these technologies can be used for ICT components that are not part of the cloud. The application of these technologies can increase availability and flexibility. This is in terms of sensor and actuator components of the smart city infrastructure. These are also important requirements if the components' possibilities of failure have to be eliminated.

ACKNOWLEDGEMENTS

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

REFERENCES

[1] Mester, G.: *Academic Ranking of World Universities 2009/2010.* Ipsi Journal Transactions on Internet Research **7**(1), 44-47, 2011, http://tir.ipsitransactions.org/2011/January/Paper%2005.pdf, accessed 1st December 2018,

[2] 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,

[3] Sostaric, D.; Horvat, G. and Hocenski, Z.: *Multi-agent Power Management System for ZigBee Based Portable Embedded ECG Wireless Monitoring Device with LabView Application.* KES-AMSTA 2012, 1-10, 2012, http://dx.doi.org/10.1007/978-3-642-30947-2_34,

[4] Mell, P. and Grance, T.: *The NIST Definition of Cloud Computing*. http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf, accessed 1st December 2018,

[5] European Commission: *A Roadmap for Advanced Cloud Technologies under H2020*. Publications Office of the European Union, Luxembourg, 2012,

[6] Calatrava, A.; Romero, E.; Moltó, G.; Caballer, M. and Alonso, J.M.: *Self-managed cost--efficient virtual elastic clusters on hybrid Cloud infrastructures*. Future Generation Computer Systems **61**(C), 13-25, 2016, http://dx.doi.org/10.1016/j.future.2016.01.018,

[7] 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,
http://www.etfos.unios.hr/ijeces/wp-content/uploads/pappers/ijeces_vol_1_no_2_01.pdf, accessed 1st December 2018,

[8] Liang, H., et al.: *vmOS: A virtualization-based, secure desktop system*.
Computers & Security **65**, 329-343, 2017,
http://dx.doi.org/10.1016/j.cose.2016.10.008,

[9] Vakili, A. and Navimipour, N.J.: *Comprehensive and systematic review of the service composition mechanisms in the cloud environments*.
Journal of Network and Computer Applications **81**, 24-36, 2017,
http://dx.doi.org/10.1016/j.jnca.2017.01.005,

[10] Ren, J.; Qi, Y.; Dai, Y.; Xuan, Y. and Shi, Y.: *Nosv: A lightweight nested-virtualization VMM for hosting high performance computing on cloud*.
Journal of Systems and Software **124**, 137-152, 2017,
http://dx.doi.org/10.1016/j.jss.2016.11.001,

[11] Hewlett-Packard Development Company: *Managing Serviceguard Twentieth Edition*.
Hewlett-Packard, 2011, HP Part Number: 5900-1869,

[12] McCabe, J.: *Introducing Windows Server 2016 Technical Preview – First Printing*.
Microsoft Press, Redmond, 2016,

[13] International Business Machines Corporation: *Introduction to Grid Computing with Globus.* 2nd edition.
IBM Redbooks, New York, 2003,

[14] Savill, J.: *Microsoft Virtualization Secrets*.
John Wiley & Sons Inc., Indianapolis, 2012,

[15] EMC Corporation: *Information Storage and Management: Storing, Managing, and Protecting Digital Information*.
John Wiley & Sons Inc., Indianapolis, 2010.