ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

https://doi.org/10.17559/TV-20220914230921

Original scientific paper

Cost and Security Aspects of the System for Monitoring and Managing Things Over the Internet

Mirko COBOVIĆ

Abstract: The use of the Internet-controlled devices has become more ubiquitous. The Internet of Things (IoT) has been developed in the sense that it is offered as a monitoring or management system but also as an ability to manage individual devices (things). Devices with already integrated connection protocols are already offered on market, as well as components that can upgrade not IoT devices. In this paper, the author examines such devices, that is, components that upgrade the already existing devices, for the purpose of managing their operation. The paper analyses the cost side of the device, where annual electricity costs are given for three IoT devices and three Internet Access Point devices for connecting devices to the Internet, i.e., to further rented services. The paper also offers an analysis of the attitudes of device users on knowledge of the possibilities, costs as well as security risks. According to the analysis, cost increases and security breaches are eligible to enable remote monitoring and management of devices.

Keywords: cost; internet of things; managing; security; survey

1 INTRODUCTION

Man, as well as society since its creation, has had a need for tools that make it easier for him to work. Initially, the tools were primitive and simple, and over time they became more complex. Complex tools, i.e., devices or things, need to be managed but also monitored for their operation. With the expansion of the Internet, control and monitoring is enabled from separate and remote locations, from one or more people and from other devices. With the advent of Cloud Computing, and especially the Internet of Things (IoT), the management and control of tools and systems has been simplified, especially because part of the infrastructure can be used as a service. The Internet of Things infrastructure [1] is composed of a range of detectors and services to operate assisted Cloud Computing. The devices themselves, in order to work, must be connected to a certain source of electricity as well as to Internet Access Point. As a rule, such devices are always active and consume a certain amount of electricity. Costs according to [2] are defined as a measure of economic efficiency, that is, according to [3] they represent the value-expressed effect of products or services. It should also be considered that the activities of the device connected to the Internet also pose a security risk, since sufficient time is left to intentionally redirect the data. Security according to [4] is the process of maintaining an acceptable risk, i.e., a measure to prevent against possible risks, threats, vulnerabilities, and damage to property.

Internet of Thing systems are increasingly implemented in various devices of home or business application. Also, Internet of Thing systems can be implemented on existing devices by upgrading Internet of Thing elements. This paper examines such Internet of Thing devices that offer to upgrade over existing not IoT devices. The cost and safety component shall be considered. The cost component is considered through the actual cost of electricity consumption over a period of one year. Furthermore, the questionnaire examined users' views on accepting costs and security risks to enable remote monitoring and management of existing devices over the Internet.

The research question that arises is: do users agree to the possibilities of remote control and monitoring of the device if security will be violated, and costs increased? According to the research question, hypotheses of the work are obtained: H1 Cost increases and security breaches are eligible to enable remote monitoring and management of devices. To refute or prove the hypothesis, two ancillary hypotheses have also been appointed: H1.1 To some extent, an increase in costs is acceptable to enable remote monitoring and management of devices and H1.2 To some extent, security breaches are acceptable to allow for remote monitoring and operation of devices.

2 RELATED WORKS

There are several papers in which the consumption and security of the Internet of Thing has been analysed. The energy consumption of Internet of Thing devices is analysed in [5] where empirical data and a framework for studying and analysing the energy flow within the system are given. Furthermore, energy consumption as well as architecture and the potential way of accessing the Internet is analysed [6] where the energy optimisation model for various data traffic systems is given. The power management model related to battery utilization was given in [7]. The paper provides a model for calculating battery life for certain ways of exploiting the system. The energy efficiency of Internet of Thing was analysed in [8] where the possibility of optimizing the energy costs of system components and automatic monitoring and control systems was presented. The paper [9] analyses the challenges and capabilities of low powered systems that connect to the Internet.

The types of security risks of computer systems that have access to the Internet were analysed in [4] where security risk eligibility measures were given. The security of the Internet of Thing system was analysed in [10] where an overview of Malware and possible risks and threats was given. Furthermore, the potential security risks of the Internet of Thing and the supporting components are analysed in [11] where proposals and solutions for safe and sustainable systems are given. Security, privacy, and trust were analysed in [12] where methods were proposed to increase the security of industrial Internet of Thing through various fields and application areas.

3 INTERNET OF THINGS

Internet of Thing is defined as "(...) a framework in which all things have a representation and a presence on the Internet. More specifically, the Internet of Things aims at offering new applications and services bridging the physical and virtual worlds, in which Machine-to-Machine communications represents the baseline communication that enables the interactions between Things and applications in the cloud." [13, 14]. Furthermore, [15] states "The Internet of Things can be treated as a superset of connecting devices that are uniquely identifiable by existing near field communication techniques. The words "Internet" and "Things" mean an inter-connected world-wide network based on sensory, communication, networking, and information processing technologies, which might be the new version of information and communications technology". Thus, the Internet of Things allows users to connect devices to the Internet for the purpose of monitoring and management. Each such device consumes a certain amount of energy and since it connects to the Internet also poses a certain security risk of the local computer network.

3.1 Cost Aspect

"Costs, in economics, represent the value of the assets spent and the real effort (resources) to produce a beneficial effect in the form of products or services." [3] Costs are necessary to obtain a beneficial effect. To facilitate the management and planning of costs, costs need to be divided. [2] For Internet of Things systems, cost-division by natural characteristics and in relation to changes in activity level are paramount. Thus, material costs arise: the cost of purchasing the device, the cost of accompanying services and the cost of electricity. As regards the division in relation to the change in activity level, there are: fixed procurement costs and variable costs of accompanying services as well as electricity costs.

3.2 Security Aspect

Security, as a process of maintaining an acceptable risk, is expressed in systems that by nature have the ability to remotely access from several devices of different users. "Computer security is a set of measures and procedures to ensure data stored in computers, often also available over a computer network" [16]. Security risks can be considered through deliberate and unintentional threats. Unintended threats are reduced by redundancy of infrastructure particularly acute in Cloud Computing systems. However, data stored in remote locations accessible over the network has a strong security risk of intentional threats. "In the case of public platforms, the question arises of the security of their own data. Applications from different users are often found on the same servers, storage systems and networks." [17] In order to reduce intentional threats as well, it is necessary to use and comply with security protocols. The systems of the Internet of Things, therefore, show that security increases due to the ability to monitor and manage, but it is also disrupted due to the possibility of access through the network.

4 INTERNET OF THINGS DEVICE-MEASUREMENT AND RESULTS

Previous chapters mentioned that the paper examines devices that offer to upgrade the capabilities of Internet of Things to already existing devices in the household and businesses. Such devices consist of a power supply, a modem for a wireless network, a microcontroller and a relay that require constant power supply as well as a permanent connection to the Internet. To calculate the cost of such a system, Internet of Things devices which can be acquired on the market were taken. These are simple devices that are easy to implement on existing devices. The specifications are listed in Tab. 1.

Table 1 Specifications of IoT devices

Device	Features	Input Voltage AC / V	Max Current AC / A	Max Power / W
IoT 1	Smart link module-1 relay	100 - 240	10	2200
IoT 2	Smart link module-1 relay	100 - 240	15	3500
IoT 3	Smart link module-4 relays	100 - 240	10	2200

To give devices access to Internet, Internet Access Point must also be provided. For measurement purposes, combined devices have been taken that can be easily implemented and acquired on the market. The specifications are listed in Tab. 2.

Table 2 Specifications of Internet AccessPoint devices

Device	Features	Input Voltage AC / V	Max. Input Current AC / A	Output Voltage DC / V	Max Output Current DC / A
IAP 1	Access Point, Router, Switch	100 - 240	1	12	2
IAP 2	Access Point, Router, Switch	100 - 240	0,6	2	2
IAP 3	Access Point, Router, Switch	100 - 240	0,3	9	0,6

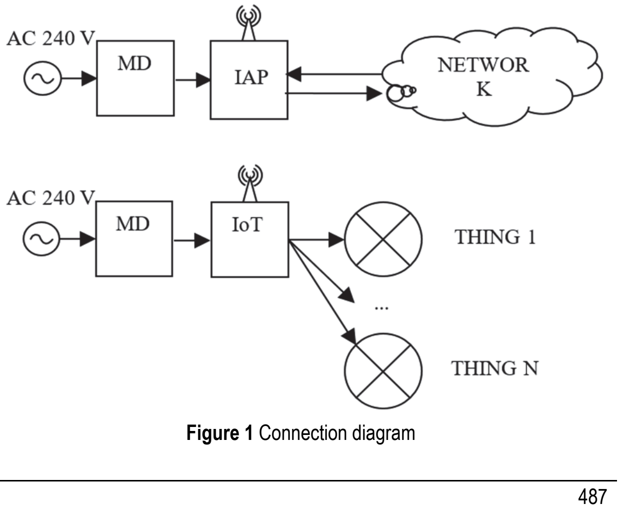

Figure 1 Connection diagram

These devices are connected according to the diagram shown by Fig. 1.

The Internet of Things device is wired to the power grid and wirelessly to Internet Access Point. Internet of Thing device as well as Internet Access Point are connected to The Measure Device (MD) to measure Voltage (*U*), Currency (*I*), and Power Factor (cos*φ*). Measure Devices VOLTCRAFT SEM4500 [18] was used for measurement, which was verified with the measured METRELEurotest 61557 [19] device.

For each device, Internet of Thing device and Internet Access Point, ten measurements were made for each condition. The state of Internet of Thing Devices is related to the turned off or turn on one, two, three or four relay. Each measurement lasted 20 minutes to stabilize all components of the system. There were no devices connected to the Internet of Thing device to obtain as accurate a consumption of the upgrade itself. Internet Access Point was connected to the Internet and to the Internet of Thing device. The Internet of Thing device was monitored using the Cloud Computing service and the service was accessed via Smartphone. In each measurement, Voltage (*U*), Current (*I*), Power Factor (cos*φ*) were measured, while Apparent Power (*S*), Active Power (*P*) and annual energy consumption for Household and Business were calculated according to [20, 21]. For the measured values, the mean ($\bar{x}$) and the standard deviation (σ) are expressed.

The results obtained for Internet of Thing devices are shown in Tab. 3 and for Internet Access Point in Tab. 4.

Table 3 Measurement and calculation data of IoT devices

Device	Relay ON		*U* / V	*I* / A	cos*φ*	*S* / VA	*P* / W	Household AC / kWh per year	Business AC / kWh per year
IoT 1	0	$\bar{x}$	241,040	0,004	0,349	0,892	0,311	2,728	7,620
IoT 1		σ	0,320	0,000	0,064				
IoT 1	1	$\bar{x}$	241,470	0,007	0,470	1,690	0,795	6,964	14,442
IoT 1		σ	0,675	0,000	0,010				
IoT 2	0	$\bar{x}$	240,610	0,004	0,334	1,035	0,346	3,030	8,840
IoT 2		σ	1,146	0,000	0,073				
IoT 2	1	$\bar{x}$	241,900	0,007	0,478	1,693	0,810	7,096	14,468
IoT 2		σ	0,966	0,000	0,013				
IoT 3	0	$\bar{x}$	242,740	0,005	0,330	1,214	0,400	3,504	10,370
IoT 3		σ	0,950	0,000	0,001				
IoT 3	1	$\bar{x}$	241,620	0,009	0,436	2,102	0,917	8,034	17,960
IoT 3		σ	1,978	0,000	0,078				
IoT 3	2	$\bar{x}$	241,940	0,012	0,448	2,903	1,300	11,388	24,806
IoT 3		σ	0,572	0,000	0,001				
IoT 3	3	$\bar{x}$	241,940	0,015	0,496	3,629	1,800	15,768	31,007
IoT 3		σ	0,624	0,000	0,001				
IoT 3	4	$\bar{x}$	242,200	0,019	0,496	4,602	2,283	19,995	39,318
IoT 3		σ	0,298	0,001	0,020				

Table 4 Measurement and calculation data of Internet Access Point

Device		*U* / V	*I* / A	cos*φ*	*S* / VA	*P* / W	Household AC / kWh per year	Business AC / kWh per year
AP 1	$\bar{x}$	241,710	0,064	0,460	15,542	7,155	62,680	132,790
AP 1	σ	1,548	0,002	0,013				
AP 2	$\bar{x}$	241,450	0,071	0,502	17,143	8,600	75,336	146,469
AP 2	σ	0,580	0,000	0,001				
AP 3	$\bar{x}$	241,800	0,021	0,512	5,078	2,600	22,776	43,385
AP 3	σ	1,054	0,000	0,002				

According to the obtained measurement results and calculations, it is evident that Internet of Thing devices consume regardless of their activity, with the relay involved on the Internet of Thing device consuming significantly more electricity than the disconnected one and increasing consumption by the number of relays included. Internet Access Point consumption is proportional to the Inputs and Outputs rated specifications. The higher the rated values, the higher the measured values.

The calculations show that power factor for Internet of Thing Device as well as for Internet Access Point is about 0,5. Due to the conversion of the alternating current of higher voltage into a direct current of lower voltage, inductive reactive energy is generated.

By the General Conditions Regulations for network use and electricity supply [20], excessive barren energy is calculated for Business, but not for Household. According to the above, and according to the calculations in Tab. 3 and Tab. 4, energy consumption is not negligible for Household and certainly not for Business.

For the calculation of the annual energy consumption of the Internet of Thing system, the principle and labelling according to the Ordinance on the labelling of household appliances was taken [22]. The annual power consumption of the device is indicated by the symbol AC. Accordingly, the annual electricity consumption of the Internet of Thing system (AC_{SioTH}) can be defined by Eq. (1).

$$AC_{SioTH} = \sum_{i=1}^{n}\left(p_{0R}\cdot AC_{IoTONi} + p_{mR}\cdot AC_{IoTOFFi}\right) + \\ +\sum_{i=1}^{n} AC_{APi} \qquad (1)$$

where: p_{0R} represents the percentage of time of turn on relays of Internet of Thing device, p_{mR} percentage of time of turn off relays of Internet of Thing Device, AC_{IoTON} represents the annual consumption of turn on relays of Internet of Thing device, $AC_{IoTOFFi}$ represents the annual consumption of turn off relays of Internet of Thing device, AC_{AP} represents the annual consumption of Internet Access Point.

Based on the Eq. (1), it is possible to determine the annual consumption for individual Internet from Thing with a certain number of components.

5 SURVEY AND RESULTS

To obtain an image of the use of the Internet of Thing and the eligibility of costs and security risks, and to refute or accept the hypothesis of the paper, a structured questionnaire collected the views of citizens. The survey questionnaire consists of three groups of questions, the first group with questions related to data about the participants' profile, another group on knowledge and use of the Internet of Thing and a third group on issues of cost and security. For the purposes of work, only the selected questions are presented. The online survey was distributed via Google Forms during 01.02.2022. to 28.2.2022. Participants, randomly selected, were guaranteed anonymity. The survey was completed by 813 participants from the territory of the Republic of Croatia. The basic data about the participants can be found in Tab. 5. The data is presented absolutely by the number of responses and relatively in percentages.

Table 5 Respondent profile

		Frequency	Percent
Gender	Man	311	38,3
	Woman	502	61,7
Age	15 - 18	5	0,6
	19 - 24	226	27,8
	25 - 49	452	55,6
	50 - 64	105	12,9
	> 64	25	3,1
Education	Secondary School	182	22,4
	Undergraduate study	283	34,8
	Graduate study	305	37,5
	Postgraduate study	43	5,3
Scientific/artistic field of your education/workplace	Natural sciences	40	4,9
	Technical sciences	269	33,1
	Biomedicine and healthcare	10	1,2
	Biotechnical sciences	15	1,8
	Social sciences	291	35,7
	Humanities	156	19,1
	Artistic area	5	0,6
	Interdisciplinary field	27	3,3

Tab. 6 presents the results of the participants. The presented answers are related to the advantages, disadvantages, costs and security risks of the Internet of Thing devices. The data is displayed using the mean ($\bar{x}$), Median and Mod and the standard deviation (σ). The deviations from the normal distribution using Skewness and Kurtosis are also presented.

Table 6 The results of the respondents

Question		$\bar{x}$	Median	Mod	σ	Skewness	Kurtosis
Do you think that the listed characteristics of devices that can connect to the Internet are advantages or disadvantages? (1 - Disadvantage, 2 - More of a disadvantage than an advantage, 3 - Neither advantage nor disadvantage, 4 - More of an advantage than a disadvantage, 5 - Advantage)	1. Acceleration of business processes.	4,77	5	5	0,545	−2,559	6,42
	2. Disease prevention.	3,69	4	3	1,159	−0,455	−0,52
	3. Improving the quality of life.	4,13	4	5	1,053	−1,214	1,064
	4. Security.	3,35	3	5	1,393	−0,291	−1,091
	5. Privacy.	2,56	2	1	1,389	0,453	−0,983
	6. Reliability.	3,37	3	3	1,133	−0,303	−0,44
	7. Purchase price.	2,94	3	3	1,197	−0,024	−0,679
	8. Total usage costs.	3,01	3	3	1,187	−0,084	−0,593
	9. Transparent communication.	3,49	3	3	1,205	−0,404	−0,597
	10. Reduced level of human interaction.	2,62	3	1	1,48	0,274	−1,307
	11. Leakage of information.	2,2	2	1	1,333	0,668	−0,794
Which reasons would be an obstacle for upgrading existing devices with control and monitoring systems via the Internet? (1 - There is no obstacle, 5 - An insurmountable obstacle)	1. Upgrade price.	3,29	3	4	1,126	−0,588	−0,214
	2. The cost of electricity of the control and monitoring system via the Internet.	2,86	3	3	1,26	−0,144	−1,071
	3. System security.	3,23	3	3	1,217	−0,37	-0,686
	4. Risk of access to the system by an unauthorized person.	3,63	4	4	1,245	−0,796	-0,302
	5. System maintenance cost.	3,22	3	4	1,184	−0,529	-0,544
Which and how much of the listed costs of using the management and monitoring system via the Internet are acceptable? (1 - Not acceptable, 2 – Acceptable if < 1%, 3 - Acceptable if < 2%, 4 - Acceptable if < 3%, 5 - Acceptable if < 4%, 6 - Acceptable if < 5%, 7 Acceptable if - 5% and more)	1. The purchase price of the system in relation to the purchase price of the upgraded device.	3,78	4	3	1,794	0,282	−0,944
	2. Increase in the cost of system electricity compared to the upgraded device.	3,54	3	3	1,792	0,381	−0,723
	3. Increasing the cost of maintaining the system compared to the device.	3,52	3	3	1,703	0,292	−0,799
Which of the characteristics would represent an advantage of upgrading existing devices with control and monitoring systems via the Internet? (1 - No advantage, 5 - Necessary advantage)	1. Ability to monitor devices from a remote location.	4,05	4	4	0,997	−1,296	1,716
	2. Ability to manage devices from a remote location.	4,2	4	5	0,875	−1,107	1,201
	3. The possibility of pairing multiple devices into one system.	3,94	4	4	0,988	−0,957	0,713
	4. Device automation.	3,93	4	4	0,928	−0,741	0,377
	5. Shutting down devices when they are not needed.	4,38	5	5	0,817	−1,411	1,913
	6. Reduction of the total cost of electricity caused by turning off devices when they are not needed	4,26	5	5	0,98	-1,363	1,309

As for the advantages and disadvantages of devices that can be connected to the Internet, the recognised advantages are Acceleration of business processes, Disease prevention and improving the quality of life; while for disadvantages they cite Privacy, Reduced level of human interaction and Leakage of information. Security, Reliability, Purchase price, Total usage costs, Transparent communication are listed as elements that represent both advantages and disadvantages. Regarding security, surveillance and management over the Internet allows faster reactions, but also poses the risk of intrusion by third, unauthorized parties. In this case, security increases due to the possibility of surveillance and control, but also distorts due to the risk of data leakage.

Barriers to upgrading existing device with control and monitoring systems over the Internet could be from the security and cost domains. The possibility of data leaks due to unauthorised access to the data processing system is cited as the biggest drawback.

In terms of costs, participants would agree to upgrades if the cost components did not exceed more than 3% of the cost of the base device.

Participants recognize the advantages after upgrading the system and see the advantage in the possibilities of shutting down the device remotely, especially when it is not in use and in terms of reducing unnecessary energy costs at those moments when the device is not in use.

6 CONCLUSION

The paper analyses certain characteristics of Internet of Things devices, especially the cost and safety component. The electricity costs of the components that make up the basic Internet of Things system were measured and calculated. According to the calculation, it is evident that the electricity costs of the system are not negligible, especially if it is Business. Based on the scheme, a mathematical term was given for the calculation of the annual electricity consumption of the Internet of Things system, which can be compared with the calculations specified in the Ordinance on the labelling of household appliances and obtained related to the consumption of individual upgrades of Internet of Things components to existing devices.

The cost component of the Internet of Things system was also examined through a questionnaire. According to the responses of participants, it can be concluded that increasing costs can justify upgrading existing devices with the capabilities of Internet of Things. Based on the participants answers, it is evident that the eligible upgrade costs are up to 3% of the cost of the upgraded device. According to the auxiliary hypothesis H1.1 To some extent, an increase in costs is acceptable to enable remote monitoring and management of devices is confirmed.

The safety component was also considered in the paper. In past research, it is possible to see that users accept security breaches if they will have the ability to remotely monitor and control devices. According to the survey, it can also be concluded that users (i.e., participants) accept to some extent security risks if the upgrade will lead to additional advantages and opportunities.

Participants report that safety has been both improved and impaired by upgrading existing devices with Internet of Things capabilities. They see advantage in the ability to control and manage, and disadvantages in possible unauthorized access to the system. According to the aforementioned auxiliary hypothesis H1.2, to some extent, security breaches are acceptable to allow for remote monitoring and operation of devices is confirmed.

By confirming auxiliary hypotheses and based on measurements, calculations and analysed attitudes of the subjects, the hypothesis of H1-Cost increases and security breaches are eligible to enable remote monitoring and management of devices - is confirmed.

For further research, it is recommended to make a cost analysis of the procurement and maintenance of IoT system components as well as security risks sampled by intentional and unintentional threats.

7 REFERENCES

[1] Panina, Ž. (2013). *Elektroničko poslovanje druge generacije*. Zagreb: Ekonomski fakultet.

[2] Karić, M. (2010). Mikroekonomika, 1. izdanje. Osijek: Ekonomski fakultet.

[3] https://www.enciklopedija.hr/Natuknica.aspx?ID=62478

[4] Cobović, M. (2021). *Računalstvo u oblaku-nove mogućnosti poslovanja*. Ekonomski fakultet, Osijek.

[5] Martinez, B., Montón, M., Vilajosana, I., & Prades, J. D. (2015). The Power of Models: Modeling Power Consumption for IoT Devices. *IEEE Sensors Journal*, *15*(10), 5777-5789. https://doi.org/10.1109/JSEN.2015.2445094

[6] Gray, C., Ayre, R., Hinton, K., & Tucker, R. S. (2015). Power consumption of IoT access network technologies. *IEEE International Conference on Communication Workshop (ICCW)*, 2818-2823. https://doi.org/10.1109/ICCW.2015.7247606

[7] Lauridsen, M., Krigslund, R., Rohr, M., & Madueno, G. (2018). An Empirical NB-IoT Power Consumption Model for Battery Lifetime Estimation. *IEEE 87th Vehicular Technology Conference (VTC Spring)*, 1-5. https://doi.org/10.1109/VTCSpring.2018.8417653

[8] Khan, Z. A. & Abbasi, U. (2018). An Energy Efficient Architecture for IoT Based Automated Smart Micro-Grid. *Tehnički vjesnik*, *25*(5), 1472-1477. https://doi.org/10.17559/TV-20160915124352

[9] Mukhopadhyay, S. C. & Suryadevara, N. K. (2014). Internet of Things: Challenges and Opportunities. *Internet of Things. Smart Sensors, Measurement and Instrumentation*, *9*. https://doi.org/10.1007/978-3-319-04223-7_1

[10] Lee, S., Jeon, H., Park, G., & Youn, J. (2021). Design of Automation Environment for Analyzing Various IoT Malware. *Tehnički vjesnik*, *28*(3), 827-835. https://doi.org/10.17559/TV-20210202131602

[11] Cha, H., Yang, H., & Song, Y. (2021). The Detection Data Processing Mechanism for Vehicular Cyber Physical System in IoT Environment. *Tehnički vjesnik*, *28*(3), 963-973. https://doi.org/10.17559/TV-20201209230220

[12] Chen, L., Ye, Z., & Jin, S. (2021). A Security, Privacy and Trust Methodology for IIoT. *Tehnički vjesnik*, *28*(3), 898-906. https://doi.org/10.17559/TV-20210122095638

[13] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The internet society (ISOC)*, *80*, 1-50.

[14] Com Soc Training. *IEEE Communications Standards Magazine*, *6*(3). https://doi.org/10.1109/MCOMSTD.2022.9927272

[15] Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: a survey. *Information systems frontiers*, *17*(2), 243-259. https://doi.org/10.1007/s10796-014-9492-7

[16] https://www.enciklopedija.hr/natuknica.aspx?ID=68380

[17] https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-03-293.pdf

[18] https://www.manualslib.com/manual/1996723/Voltcraft-Sem4500.html?page=66#manual

[19] https://www.manualslib.com/products/Metrel-Eurotest-61557-8700839.html
[20] https://narodne-novine.nn.hr/clanci/sluzbeni/2022_08_100_1473.html
[21] Krčum, P. (2012). *Električna mjerenja*. Sveučilište u Splitu, Split.
[22] https://narodne-novine.nn.hr/clanci/sluzbeni/2007_12_130_3718.html

Contact information:

Mirko COBOVIĆ, PhD
(Corresponding author)
University of Slavonski Brod
Trg Ivane Brlić Mažuranić 2, 35000 Slavonski Brod, Croatia
E-mail: mcobovic@unisb.hr