UDC 004
21.3
681.5
In print: ISSN 2545 – 4250
On line: ISSN 2545 – 4269

JOURNAL OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGIES

СПИСАНИЕ ЗА ЕЛЕКТРОТЕХНИКА И ИНФОРМАЦИСКИ ТЕХНОЛОГИИ

J. Electr. Eng. Inf.. Technol.	Vol.	No.	pp.	Skopje
	9	1	1–74	2024
Спис. Електротехн. Инф. Технол.	Год.	Број	стр.	Скопје

J. Electr. Eng. Inf.. Technol.	Vol.	No.	pp.	Skopje
	9	1	1–74	2024
Спис. Електротехн. Инф. Технол.	Год.	Број	стр.	Скопје

JOURNAL OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGIES
СПИСАНИЕ ЗА ЕЛЕКТРОТЕХНИКА И ИНФОРМАЦИСКИ ТЕХНОЛОГИИ

Published by:
Faculty of Electrical Engineering and Information Technologies, "Ss. Cyril and Methodius" University in Skopje, P.O.Box 574, MK-1001 Skopje, North Macedonia

Издава:
Факултет за електротехника и информациски технологии, Универзитет „Св. Кирил и Методиј" во Скопје, пошт. фах 574, МК-1001 Скопје, Северна Македонија

Published twice yearly – Излегува два пати годишно

Address Адреса
http://jeeit.feit.ukim.edu.mk
jeeit@feit.ukim.edu.mk

JEEIT is indexed/abstracted in INIS (International Nuclear Information System)

JOURNAL OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGIES
СПИСАНИЕ ЗА ЕЛЕКТРОТЕХНИКА И ИНФОРМАЦИСКИ ТЕХНОЛОГИИ

J. Electr. Eng. Inf.. Technol.	Vol.	No.	pp.	Skopje
	9	1	1–74	2024
Спис. Електротехн. Инф. Технол.	Год.	Број	стр.	Скопје

TABLE OF CONTENTS
(С О Д Р Ж И Н А)

Metrology – Метрологија

Automation – Автоматика

Electrical Energy – Електроенергетика

Telecommunications – Телекомуникации

Journal of Electrical Engineering and Information Technologies, Vol. **9,** No. 1, pp. 5–12 (2024)
Article 214
Received: May 15, 2024
Accepted: May 31, 2024
In print: ISSN 2545–4250
On line: ISSN 2545–4269
UDC: 621.317.78.088.3
https://doi.org/10.51466/JEEIT2491214005v

Original scientific paper

INTERLABORATORY COMPARISONS OF THE CALIBRATION RESULTS OF ENERGY METERS

Oleh Velychko[1]*, **Yulia Kulish**[1], **Boris Gendelman**[3]

[1]*State Enterprise "All-Ukrainian State Research and Production Center for Standardization, Metrology, Certification and Consumers Rights Protection", 4 Metrologichna Str., 03143 Kyiv, Ukraine*
[2]*SATEC Calibration Lab., 25 Zeev Lev Str., 9145001, Jerusalem, Israel*
*velychko@hotmail.com

A b s t r a c t: The article is devoted to the analysis of the results of the interlaboratory comparison (ILC) of the electric energy meter, which were carried out in 2024. ILC results of calibration of the energy meter at the points of alternating voltage 230 V, currents from 0.05 A to 10 A, power factors from ±1.0 to ±0.5 at a frequency of 50 Hz are presented. The deviations of the results obtained by each laboratory were determined, and the consistency of the obtained results was assessed, taking into account the uncertainty of the measurements using the criterion of functioning statistics. In general, laboratories have received satisfactory accuracy and there is good agreement between participants for this quantity. Laboratories meet the established requirements and confirms their qualification (technical competence) during the calibration in accordance with the requirements of the standard ISO/IEC 17025. It is expected that this ILC will be able to provide support for participants' calibration capabilities.

Key words; calibration; energy meter; interlaboratory comparison; uncertainty

МЕЃУЛАБОРАТОРИСКА СПОРЕДБА НА РЕЗУЛТАТИ ОД КАЛИБРАЦИЈА НА БРОИЛА ЗА ЕЛЕКТРИЧНА ЕНЕРГИЈА

А п с т р а к т: Трудот е посветен на анализата на резултатите од меѓулабораториската споредба (ILC) на броилата за електрична енергија, која беше направена во 2024 година. Прикажани се резултатите од споредбата за напон од 230 V, струи од 0,05 A до 10 A, факторите на моќност од ±1,0 до ±0,5, при фреквенција од 50 Hz. Утврдени се отстапувања на резултатите добиени од секоја лабораторија и оценета е конзистентноста на добиените резултати, земајќи ја предвид мерната неодреденост. Генерално, лабораториите добија задоволителна точност и постои добро совпаѓање на добиените резултати. Лабораториите ги исполнуваат утврдените барања и ја потврдуваат нивната квалификација (техничка компетентност) за калибрацијата во согласност со барањата на стандардот ISO/IEC 17025. Се очекува дека меѓулабораториската споредба ќе придонесе за развојот на калибрациските капацитети на двете лаборатории.

Клучни зборови: калибрација; броило за електрична енергија; меѓулабораториска споредба; мерна неодреденост

1. INTRODUCTION

Electrical energy measurement is important for a variety of purposes, including: calculating electricity consumption; consumption management; diagnostics and network support; research and development, etc. For commercial and residential users, energy measurement allows one to accurately calculate the cost of used electricity. For industrial enterprises or power supply networks, it is important to measure energy for effective consumption management, resource planning and optimization of production processes. Monitoring power consumption helps to detect anomalies that may indicate network problems, such as overloads or faults. Energy measurement is also used in scientific research and development of new technologies to improve energy efficiency and create new energy sources.

Interlaboratory comparisons (ILCs) are the process of comparing the results of measurements

made in different laboratories in order to assess and confirm the accuracy, reliability and reproducibility of measurements. They have several important meanings: validation of measurement methods; evaluation of measurement standards and measuring instruments; confirmation of mutual acceptability of results; increasing confidence in measurement results; data quality assurance, etc. Comparing results between different laboratories helps to determine the effectiveness and reproducibility of used standards and measuring instruments. ILCs contribute to the improvement of the data quality control system and help to identify possible sources of error or discrepancies in measurements. The ILC results can contribute to increasing confidence in the data obtained in measuring laboratories and provide greater objectivity and reliability of measurements.

Confirmation of the competence of laboratories is an important process for ensuring the quality and reliability of measurement results. The main stages of this process include: accreditation as the first step in confirming competence; participation in ILCs; laboratory quality system; periodic inspection and calibration of measurement equipment to ensure the required accuracy of measurements; assessment of personnel qualifications; internal and external audits, etc. Together, these steps ensure a high level of competence of the laboratories in the performance of their functions and ensure the reliability and objectivity of the results of their activities.

ILC is one of the forms of experimental verification of the activity of laboratories with the aim of determining technical competence in a certain type of activity. A laboratory can participate in ILC programs, where its measurement results are compared with the results of other laboratories. This helps to assess the accuracy and reliability of its measurement methods. Successful ILC results for the laboratory are confirmation of competence in carrying out certain types of measurements by a specific specialist on specific equipment. National agencies for the accreditation of laboratories have established strict requirements for participation in the relevant ILCs, in particular for calibration laboratories (CL) for each type of measurement and each type of measurement value, which are included in the scope of laboratory accreditation.

2. RELATED PAPERS

Publications devoted to issues of organization of ILCs and methods of processing the received data in specific types of measurement or test are of considerable interest. The ILC program is developed taking into account the requirements of international standards ISO/IEC 17025 [2], ISO/IEC 17043 [1], ISO 13528 [3]. Improvement of the methods of processing ILC results is necessary to obtain reliable ILC results. Unsatisfactory ILC results can be associated not only with a deviation from the normal state of competence of the laboratory, but also with malfunctions of the equipment available in the laboratory or insufficient competence of the specialist who worked with it.

Scientific publications deal with a number of important issues regarding conducting ILC for CL, which mainly relate to the specifics of calibration for certain types of measurements. Algorithms and results of ILCs are given in works [4–8] for the purpose of evaluating the measuring capabilities of laboratories and obtaining highly accurate and precise data. Approaches for improvement of measurement methods and uncertainty assessment of ILC participating laboratories for various types of measurements (pressure, water flow, active power, temperature) are considered in [9–12]. Evaluation of the results of laboratories that participated in ILCs on specific types of measurements (reactive power, length, pressure) are presented in [13–15].

3. PROBLEM STATEMENT

The purpose of the carried-out research was to process the data received from ILC participating laboratories and compare them.

To achieve the set goal, it is necessary to solve the following problems:

– to research the calibration item for the ILC of energy meters, determine the assigned value and its extended uncertainty of this ILC;

– to calculate the degree of equivalence for each of the ILC participating laboratories and their expanded uncertainties;

– to evaluate the results of the calibration by participating laboratories of the ILC, taking into account the criteria of functioning statistics.

4. OVERVIEW OF THE INTERLABORATORY COMPARISON RESULTS

ILC for calibration of energy meter (UMTS-ILC-E:2024) was conducted from February to April 2024. In this ILC two laboratories carried out: State Enterprise “All-Ukrainian State Research and Production Center for Standardization, Metrology, Certification and Consumers Rights Protection” (SE “Ukrmetrteststandard” – UMTS, Ukraine), and SATEC Calibration Lab. (Israel). UMTS is accre-

dited of the National Accreditation Agency of Ukraine (NAAU), Calibration No. 40004. SATEC Calibration Lab. is accredited of the Israel Laboratory Accreditation Authority (ISRAC), Calibration No. 357. NAAU and ISRAC are one of the signatories of the International Accreditation Cooperation (ILAC) arrangement for the mutual recognition of calibration results.

UMTS was selected as the referent laboratory (RL). Dr. Oleh Velychko was the ILC coordinator. The RL is responsible for providing the calibration item (CI) for ILC, coordinating the schedule, collecting and analyzing the comparison data, preparing the draft of report, etc. The ILC program was developed taking into account the requirements of international standards ISO/IEC 17025 [2], ISO/IEC 17043 [1] and ISO 13528 [3]. ILC was carried out in accordance with ISO/IEC 17025 standard to confirm the competence of accredited calibration laboratories.

Selected CI is SATEC EM133-XM(SE) 5A, an self-energized version of EM133 energy meter, serial number 40004123. SATEC EM133 is an energy meter family, ideal for a wide range of applications such as revenue active/reactive multi-tariff energy metering (Time of Use tariff system), industrial power monitoring and for interfacing SCADA in utility substations – with direct & indirect (transformer operated) measuring connection. Based the SATEC PM13X family functionality, it is a version designed as DIN-rail mount, equipped with built-in communication ports, digital I/Os and antitamper enclosures. The family comprises of meters with direct connection (up to 63 A) and transformer operated application (up to 10 A); self-energized (SE) and auxiliary power supply versions. More information of the EM133 is available at [16].

Meter chosen for comparison has 5A nominal measured current/10A max current is intended for transformer-operated applications (connection to High Voltage power lines).

Main characteristics of EM133-XM(SE)-5A (self-energized version, powered from measured voltages):

– measured voltage/supply voltage 57/100-277/480 V (L-L/L-N);
– measurement frequency range for voltage 25–400 Hz;
– current rating direct up to 10 A;
– current burden for 10 A < 0.4 VA;
– voltage burden (total) 5 VA;
– frequency range measurement 50/60 Hz;
– operational range of temperature –25°C to 60°C;
– dimensions 125 × 90 × 75 mm.

Appearance of EM133-XM(SE)-5A is shown on Figure 1.

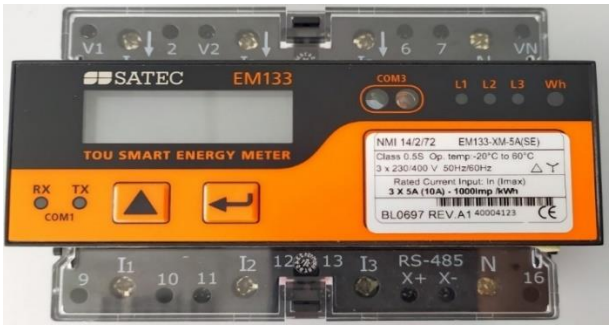


Fig. 1. Appearance of EM133-XM (SE)-5A

Main measurements should be performed with the input signals and environmental conditions:

– AC voltage 230 V ± 0.05 %;
– current from 0.05 to 10 A ± 0.05 %;
– power factor (PF) 1.0, ±0.5;
– frequency 50 ± 0.01 Hz;
– ambient temperature 22 ± 3 °C;
– relative humidity 40 ± 3 %.

UMTS as a basis for the AC power standard uses National AC Power Measurement Standard of Ukraine (NDETU EM-08-2023), which consists of a reference standard COM 3003 ZERA AC energy and a Highly Stable Power Source. This measurement setup is usually for calibration service. A block diagram of the measurement setup of the UMTS AC energy measurement is shown in Figure 2.

The operating principle is based on comparing the measured energy values of the reference standard COM 3003 ZERA and the device under test (DUT) SATEC EM133 electric energy meter. Using a reference generator, the highly stable voltage and current signals were applied to the reference standard and the electric energy meter with the setting of the corresponding phase shifts between them. Voltage and current connection scheme is three-phase, star (WYE).

With the help of the measuring head, which is connected to the reference standard, the numbers of pulses of the electric energy meter, which are proportional to the corresponding measured value of electric energy for a certain period of time, were scanned. These pulses were compared with the reference pulses, which are proportional to the measured value of electrical energy using the reference standard. The errors and standard deviation of the electrical energy readings were calculated with the help of software of NDETU EM-08-2023.

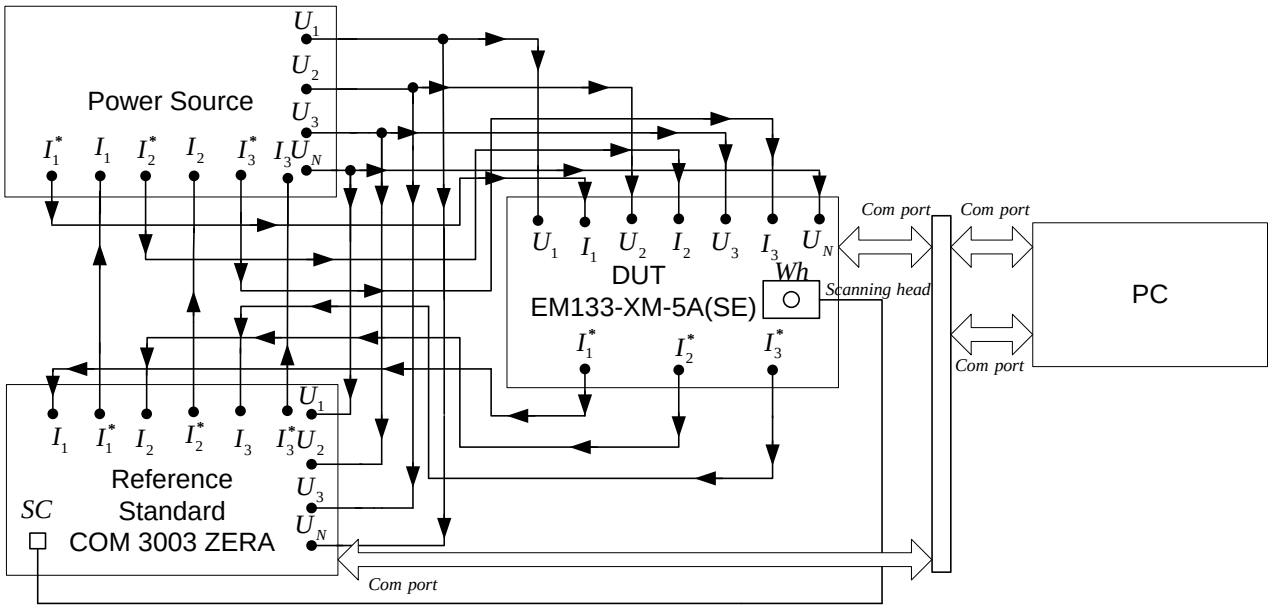


Fig. 2. Simplified schematic diagram of the measurement setup of the UMTS

The full measurement report of UMTS and SATEC contained all relevant data and uncertainty estimates. The reports included a description of the measurement method, the traceability to the SI, and the results and associated uncertainties. The calibration errors x_i and their expanded uncertainties $U(x_i)$ reported by the laboratories are given in Table 1 for AC voltage 230 V at frequencies of 50 Hz.

T a b l e 1

Calibration results of measurement of electric energy for laboratories

Current A	PF	Flow positive/negative	Calibration error x_i %		Uncertainty $U(x_i)$ %	
			UMTS	SATEC	UMTS	SATEC
0.05	1.0	Positive	–0.06	–0.055	0.049	0.049
0.5			–0.02	–0.029	0.047	0.036
5			–0.021	–0.031	0.046	0.036
10			–0.044	–0.054	0.046	0.036
0.5	0.5	Positive	0.077	0.092	0.044	0.05
5			–0.03	–0.033	0.045	0.05
10			–0.108	–0.067	0.044	0.05
5	1.0	Negative	–0.023	–0.032	0.046	0.036
10			–0.045	–0.056	0.045	0.036
5	0.5	Negative	–0.033	–0.041	0.044	0.05
10			–0.115	–0.101	0.045	0.05

5. RESULTS OF THE ANALYSIS

UMTS was a pilot laboratory of COOMET key comparison of power (COOMET. EM-K5) [18], and GULFMET supplementary comparison of AC energy (GULFMET. EM-S5) [19], responsible for providing the travelling standard, coordinating the schedule, collecting and analyzing the comparison data, and preparing the draft report.

The uncertainty was calculated following the GUM [17]: standard uncertainties, degrees of freedom, correlations, scheme for the uncertainty evaluation. All contributions to the uncertainty of measurement were listed separately in the report and identified as either Type A or Type B uncertainties. The overall uncertainty, as calculated from the individual uncertainties, was stated.

Uncertainties were evaluated at the level of one standard uncertainty. The main uncertainty components were expected: experimental standard uncertainty of the mean of *N* independent measurements; uncertainty in the primary standard or working standard against which the CI is measured; uncertainty due to leads correction. Participants included additional sources of uncertainty too.

The uncertainty budget for the UMTS reference for PF = 1.0, AC current of 0.05 A, AC voltage of 230 V at frequency of 50 Hz is presented in Table 2.

The ILC assigned values (AV) X_{AV} are calculated as the mean of participant data:

$$X_{AV} = \frac{(x_{\mathrm{UMTS}} + x_{\mathrm{SATEC}})}{2} \qquad (1)$$

$$U(X_{AV}) = 2\sqrt{\frac{1}{\left(\frac{1}{u^2(x_{\mathrm{UMTS}})} + \frac{1}{u^2(x_{\mathrm{SATEC}})}\right)}}, \qquad (2)$$

where x_{UMTS} and x_{SATEC} are measurement error for UMTS and SATEC, accordingly, $u(x_{\mathrm{UMTS}})$ and $u(x_{\mathrm{SATEC}})$ are combined standard uncertainty for UMTS and SATEC, accordingly.

Assigned values with expanded standard uncertainties is given for AC voltage of 230 V and frequency of 50 Hz in Table 3. Only one value is reported for laboratories. Degrees of equivalence (DoE) of the laboratories are reported for AC voltage of 230 V at frequencies of 50 Hz.

The DoE of *i*-th laboratory with expanded uncertainties with respect to the AV is estimated as

$$D_{lab\,i} = x_{lab\,i} - X_{AV}, \qquad (3)$$

$$U(D_{lab\,i}) = \sqrt{U^2(x_{lab\,i}) + U^2(X_{AV})}. \qquad (4)$$

DoE with expanded uncertainties for laboratories for AC voltage 230 V at frequencies of 50 Hz are given in Table 4.

T a b l e 2

The uncertainty budget for the UMTS for PF = 1.0, AC current of 0.05 A, AC voltage of 230 V at frequencies of 50 Hz

i	Quantity (unit)	Distribution	x_i	$u(x_i)$, %	v_i	c_i	$u_i(y)$, %
1	Standard deviation of the relative mean value of the observation of the differences between the value energy meter and the reference standard	normal	–0.059	0.010	4	1	0.010
2	Correction due to the accuracy of reproduction of the voltage by the power source	rectangular	0	0.014	∞	1	0.014
3	Correction due to the accuracy of reproduction of the current strength by the power source (PS)	rectangular	0	0.014	∞	1	0.014
4	Correction due to the accuracy of the electrical energy measurement by the reference standard COM 3003 ZERA	normal	0	0.005	∞	1	0.005
5	Correction due to the accuracy of the frequency internal generator of impulse signals of the COM 3003 ZERA for energy comparison	normal	0	$5\cdot10^{-5}$	∞	1	$5\cdot10^{-5}$
6	Correction determined by the stability of voltage reproduction by the PS	normal	0	0.005	∞	1	0.005
7	Correction determined by the stability of current reproduction by the PS	normal	0	0.005	∞	1	0.005
8	Drift of the reference standard COM 3003 since the last calibration	normal	–0.0017	0	∞	1	0
y	Combined standard uncertainty, %						0.024
	Expanded uncertainty (95 %, k = 2), %						0.049

Table 3

AV and expanded uncertainties of AV for AC voltage of 230 V at frequencies of 50 Hz

Current A	PF	Flow positive/negative	AV X_{AV} %	Uncertainty $U(X_{AV})$ %
0.05	1.0	Positive	–0.058	0.0346
0.5			–0.026	0.0286
5			–0.027	0.0284
10			–0.050	0.0284
0.5	0.5		0.084	0.0330
5			–0.031	0.0334
10			–0.090	0.0330
5	1.0	Negative	–0.029	0.0284
10			–0.052	0.0281
5	0.5		–0.036	0.0330
10			–0.109	0.0334

Table 4

DoE with expanded uncertainties for laboratories

Current A	PF	Flow positive/negative	DoE $D_{tab\ i}$ %		Uncertainty of DoE $U(D_{lab\ i})$ %	
			UMTS	SATEC	UMTS	SATEC
0.05	1.0	Positive	0.000	0.003	0.0600	0.0600
0.5			0.006	–0.003	0.0550	0.0460
5			0.006	–0.004	0.0540	0.0458
10			0.006	–0.004	0.0540	0.0458
0.5	0.5	Positive	–0.007	0.008	0.0550	0.0599
5			0.001	–0.002	0.0561	0.0602
10			–0.018	0.023	0.0550	0.0599
5	1.0	Negative	0.006	–0.003	0.0540	0.0458
10			0.007	–0.004	0.0531	0.0457
5	0.5		0.003	–0.005	0.0550	0.0599
10			–0.006	0.008	0.0561	0.0602

6. RESULTS OF THE ANALYSIS

The criterion of functioning statistics – the E_n number is chosen for the analysis of the obtained results of the ILC and the formation of conclusions about the laboratories.

Additionally, the performance E_n number is calculated as:

$$E_{n\ lab\ i} = 2\frac{|D_{lab\ i}|}{U(D_{lab\ i})} \leq 1.0. \quad (5)$$

E_n number for laboratories for AC voltage of 230 V at frequencies of 50 Hz are given in Table 5. Laboratories meet the established requirements for E_n number ($|E_n| \leq 1.0$): UMTS – from 0.00 to 0.33; SATEC – from 0.04 to 0.39.

T a b l e 5

DoE with expanded uncertainties for laboratories

Current A	PF	Flow positive/negative	E_n for UMTS	E_n for SATEC
0.05	1.0	Positive	0.00	0.04
0.5			0.10	0.07
5			0.11	0.08
10			0.11	0.08
0.5	0.5		0.12	0.14
5			0.02	0.03
10			0.33	0.39
5	1.0	Negative	0.10	0.07
10			0.13	0.09
5	0.5		0.06	0.08
10			0.11	0.13

7. CONCLUSION

A ILC of active and reactive energy meter at the points of alternating voltage of 230 V, currents from 0.05 A to 10 A, power factors from ±1.0 to ±0.5 at a frequency of 50 Hz has been conducted between participating calibration laboratories from Ukraine and Israel. In general, laboratories have received satisfactory accuracy and there is good agreement between participants for this quantity. Laboratories meet the established requirements for E_n number ($|E_n| \leq 1.0$) and confirms the its qualification (technical competence) during the calibration in accordance with the requirements of the standard ISO/IEC 17025. It is expected that this ILC will be able to provide support for participants' calibration capabilities.

REFERENCES

[1] ISO/IEC 17043 (2023): Conformity assessment – General requirements for the competence of proficiency testing providers, *ISO/IEC* [Online]. Available: https://www.iso.org/standard/80864.html

[2] ISO/IEC 17025 (2017): General requirements for the competence of testing and calibration laboratories, *ISO/IEC* [Online]. Available: https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html

[3] ISO 13528 (2022): Statistical methods for use in proficiency testing by interlaboratory comparison, *ISO* [Online]. Available: https://www.iso.org/standard/78879.html

[4] Claudio, J., Costa. M. (2012): Brazilian energy interlaboratory program applicative, *XX IMEKO World Congress "Metrology for Green Growth*", Busan, Republic of Korea, 6 p. [Online]. Available: https://www.imeko.org/publications/wc-2012/IMEKO-WC-2012-TC4-P5.pdf

[5] Sandu, I., Dragomir, L., Pantelimon, B. (2007): Interlaboratory comparison, *15th IMEKO TC 4 Symposium on Novelties in Electrical Measurements and Instrumentations*, Iasi, Romania, 4 p. [Online]. Available: https://www.imeko.org/publications/tc4-2007/IMEKO-TC4-2007-179.pdf

[6] Sousa, J. J. L., Leitão, L. T. S., Costa, M. M., Faria, M. C. (2012): Considerations on the influence of travelling standards instability in an interlaboratory comparison program, *XX IMEKO World Congress* "*Metrology for Green Growth*", Busan, Republic of Korea, 4 p. [Online]. Available: https://www.imeko.org/publications/wc-2012/IMEKO-WC-2012-TC8-O2.pdf

[7] Velychko O. et al. (2018): Interlaboratory comparisons of the calibration results of time meters, *Eastern-European Journal of Enterprise Technologies, Information and Controlling Systems* **1/9** (91), pp. 4–11. doi: https://doi.org/10.15587/1729-4061.2018.121089

[8] Velychko, O., Gordiyenko, T. (2022): The data evaluation of interlaboratory comparisons for calibration laboratories, *Applied Aspects of Modern Metrology*, IntechOpen. doi: https://doi.org/10.5772/intechopen.99489

[9] Bermanec, L. G., Zvizdic, D. (2015): Interlaboratory comparison in the pressure range from 0 to 2 MPa for accredited calibration laboratories, *Int. J. Metrol. Qual. Eng*. **6** (3), p. 307. doi: https://doi.org/10.1051/ijmqe/2015021

[10] Furuichi, N. et al. (2016): Inter-laboratory comparison of small water flow calibration facilities with extremely low uncertainty, *Measurement*, Vol. **91**, pp. 548–556, doi: https://doi.org/10.1016/j.measurement.2016.05.088

[11] Poenaru, M. M. et al. (2016): Active power quality assessment through interlaboratories comparison, *21th IMEKO TC4 International Symposium* "*Understanding the World through Electrical and Electronic Measurement*", Budapest, Hungary, pp. 224–228. [Online]. Available: https://www.imeko.org/publications/tc4-2016/IMEKO-TC4-2016-42.pdf

[12] Petkova, T. P. et al. (2013): Assessing technical competence through participation in interlaboratory mergers, *Information Processing Systems*, No. **3** (110), pp. 82–85. [Online]. Available: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=soi_2013_3_21

[13] Iacobescu, F., Poenaru, M. M., Anghel, M.-A. (2017): Reactive power quality assessment through interlaboratories comparison, *22th IMEKO TC 4 Symposium* "*Supporting World Development through Electrical and Electronic Masurements*", Iasi, Romania, pp. 13–19. [Online]. Available: https://www.imeko.org/publications/tc4-2017/IMEKO-TC4-2017-003.pdf

[14] Poenaru, M. M., Iacobescu, F., Anghel, M.-A. (2017): Length calibration quality assessment through interlaboratories comparison, *22th IMEKO TC 4 Symposium "Supporting World Development through Electrical and Electronic Measurements"*, Iasi, Romania, , pp. 20–26. [Online]. Available: https://www.imeko.org/publicatio ns/tc4-2017/IMEKO-TC4-2017-004.pdf

[15] Poenaru, M. M., Iacobescu, F., Anghel, M.-A. (2017): Pressure calibration quality assessment through interlaboratories comparison, *22th IMEKO TC 4 Symposium "Suporting World Development through Electrical and Electronic Mmeasurements"*, Iasi, Romania, pp. 27–32. [Online]. Available: https://www.imeko.org/publications/tc4-2017/I MEKO-TC4-2017-005.pdf

[16] EM133 Datasheet, *SATEC Ltd*., 2022, 8 p. [Online]. Available: https://www.satec-global.com/wp-content/uploads/2022/11/EM133-Datasheet.pdf

[17] JCGM 100 (2008): Evaluation of measurement data – Guide to the expression of uncertainty in measurement, *JCGM*. [Online]. Available: https://www.bipm.org/documents/20126/2071204/JCGM100_2008_E.pdf/cb0ef43f-baa5-11cf-3f85-4dcd86f77bd6

[18] Velychko, O., Karpenko, S. (2019): Final report on COOMET key comparison of power (COOMET. EM-K5), *Metrologia*, Vol. **56**, Issue 1A, 01010, doi: https://doi.org/10.1088/0026-1394/56/1A/01010

[19] Velychko O., et al. (2020): Final report on GULFMET supplementary comparison of AC energy (GULFMET. EM-S5), *Metrologia*, Vol. **5**7, Issue 1A, 01003, doi: https://doi.org/10.1088/0026-1394/57/1A/01003

Journal of Electrical Engineering and Information Technologies, Vol. **9,** No. 1, pp. 13–20 (2024)
Article 215
Received: December 6, 2023
Accepted: December 30, 2023
In print: ISSN 2545–4250
On line: ISSN 2545–4269
UDC: 004.896:[681.586:514.84-023.251
https://doi.org/10.51466/JEEIT2491215013d

Original scientific paper

DESIGN OF CARTESIAN ROBOT TEST RIG FOR ANGULAR POSITION SENSORS

Filip Dončevski, Duško Stavrov, Gorjan Nadžinski, Mile Stankovski

Faculty of Electrical Engineering and Information Technologies,
Ss. Cyril and Methodius University in Skopje,
18 Rugjer Bošković Str., 1000 Skopje, Republic of North Macedonia
fdoncevski@feit.ukim.edu.mk) // milestk@feit.ukim.edu.mk)

A b s t r a c t: A design solution for a test rig is proposed, intended for experimentation with angular position sensors. The test rig utilizes a Cartesian robot (gantry robot) with an additional axis for the purpose of implementing rotational motion. In addition, this test rig introduces a supervisory control system (SCS) for the purpose of: interacting with the user, acquiring and recording measurement results from an oscilloscope, coordination between the motion of robot and oscilloscope measurement actions. The test rig will provide a remote access with real-time video stream that will enable control and monitoring activity from Wide Area Network (WAN). The design incorporates a goal of a low cost build while achieving a reasonable motion accuracy for the testing purposes of a common angular position sensor. Furthermore, the build is designed to be modular and flexible enough to be repurposed for future educational uses in the field of robotics. The design envisages a solution that should require the least amount of custom developed technologies, utilizing already available and widely used mechanical and electrical hardware components, as well as software tools and libraries.

Key words: test rig; Cartesian robot; XYZR robot; angle sensor; inductive sensor; eddy-currents

ПРОЕКТИРАЊЕ НА ЕКСПЕРИМЕНТАЛНА ПЛАТФОРМА СО ДЕКАРТОВ РОБОТ ЗА ТЕСТИРАЊЕ НА СЕНЗОРИ ЗА МЕРЕЊЕ АГОЛНА ПОЗИЦИЈА

А п с т р а к т: Претставено е проектирано решение за експериментална платформа наменета за експериментирање со сензори за мерење аголна позиција. Експерименталната платформа користи Декартов робот со дополнителна оска за имплементирање на кружно движење. Претставен е систем за надзорно управување (СНУ) со намена: комуникација со корисникот, прибирање и зачувување мерни резултати од осцилоскоп, координација помеѓу движењето на роботот и мерните дејства на осцилоскопот. Експерименталната маса нуди далечински пристап со видео-приказ во реално време, така што се овозможуваат управувачки и надзорни активности од регионална мрежа (WAN). Проектот нуди економично решение со задоволителна прецизност во движењето на роботот, применливо за најчесто користените сензори за аголна позиција. Дополнително, решението е проектирано да биде модуларно и доволно флексибилно за идна пренамена за образовни цели во полето на роботиката. Проектот е предвиден да користи минимален број посебно изработени технологии, така што ќе искористи веќе пристапни и широко користени машински и електрични хардверски компоненти, софтверски алатки и библиотеки.

Клучни зборови: експериментална платформа; Декартов робот; робот XYZR; аголен сензор; индуктивен сензор; вртложни струи

1. INTRODUCTION

The automotive industry faces novel and innovative sensor solutions on a consistent basis, as a result of the gradual and undeniable transition towards electric vehicles (EVs). The demand for innovation and development in the EV industry has led to a development and requirement for new type of sensors and actuators. Robust and low cost angle sensors, with acceptable accuracy, are unquestionable necessity in the automotive industry with wide applications for throttle positioning, steering wheel sensing, pedal

position sensing, electric motor control [1–3]. Many of these sensors utilize different sensing techniques such as [4]: capacitive, inductive, hall-effect or optical angle sensors.

Among these sensors, an inductive eddy-current type of sensor with planar coils has taken space in the automotive market [5–10]. This type of sensor is not affected by contamination like dust, moisture, grease, oil, or other materials as long as they are non-magnetic. Furthermore these sensors provide considerable robustness to variable temperature conditions and mechanical vibrations which are common in the automotive environment. Finally, the ease of manufacturing and low cost makes these sensors a very viable solution for the automotive industry. Multiple designs of sensors have been suggested in the literature [11–17] that were based on this working principle and this work is intended for the development and research of one such sensor.

Namely, a design solution for a test rig shall be suggested with the intention of experimentation with an angular position sensor. The proposed test rig should allow for executing automatic test measurements on the sensor for variable rotational and translational displacements. Consequently the acquired measurement data will enable analysis and optimization of the sensor during research and development. Novel research work on angular position sensors is omnipresent in the field, however rarely do the authors mention the details related to the utilized test rig intended for performing tests on the sensor. A design of a Cartesian robot is presented in several works [24–27], however its utilization does not encompass a test rig for angular position sensors. To the best of our knowledge, a detailed design solution for such a testrig has not been covered by present literature, therefore the aim of this work is to put forward the intricacies of said design.

For this purpose, a Cartesian robot is proposed with an additional axis for executing rotational motion in the sensor. The Cartesian configuration of the robot was determined to be the most appropriate solution because of its ease of use and widely available software libraries for motion control. Considering the simplicity of a decentralized multi-joint control [18], which is applicable in this type of configuration, control of the whole robot is based on individual single-joint control for each axis. Furthermore, this type of configuration is utilized pervasively in the industry through various applications such as: pick and place, material handling and packaging, laboratory experiments, assembly, and other applications in manufacturing [19]. In addition, the test rig shall provide a remote access for control and monitoring activities from WAN being mediated from a supervisory control system (SCS) which will also coordinate between motion of the robot and measurement actions of the test rig.

This paper is organized as follows. In Section 2 the utilization purpose of the test rig and design goals are presented. In Section 3 the proposed mechanical design is described. The necessary details in regards to electrical and software design are provided in Section 4. In Section 5, the main conclusions are drawn along with plans for future work.

2. TEST RIG PURPOSE

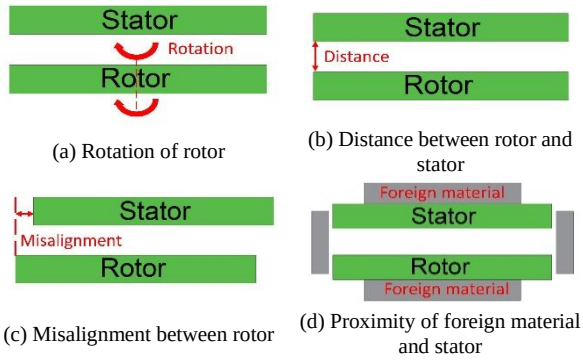
a) *Requirements*

Most contactless angle sensors are comprised of two parts: stator and rotor. The stator is the active part of the sensor which most commonly contains the electrical circuits for providing angular measurement output while the rotor is the moving part that passively causes changes in the measured signals. The intended purpose of the test rig is to implement precise rotational motion in the rotor so as to perform measurements of the signals obtained for different angular displacements. However apart from rotational displacement, non-contact angle sensors can demonstrate different output results for XYZ displacements in the Cartesian space as well. Considering that the rotor and stator almost never experience an ideal mechanical arrangement in practical implementation, it is important for the test rig to provide testing ability for such cases.

Namely, a displacement in the Cartesian space may provide information in regards to: signal strength, measurement sensitivity, influence and susceptibility to errors due to mechanical sensor arrangement, influence of different types of materials in nearby proximity, optimal mechanical placement of stator and rotor, etc. Figure 1 illustrates different possible examples of test cases with an angular position sensor.

Robot motion in the Cartesian space should be as precise as possible in order to achieve reproducible measurement results. Furthermore, it is required from the test rig to coordinate motion of the robot in accordance with the obtained measurements. Consequently, each incremental motion of the robot should be realized only after the measurement results have been obtained for the appropriate angle.

This allows for proper designation of each measurement according to the position of the rotor in relation to the stator.



(a) Rotation of rotor

(b) Distance between rotor and stator

(c) Misalignment between rotor

(d) Proximity of foreign material and stator

Fig. 1. Various test cases for an angular position sensor

In addition, a remote access to the test rig will provide additional ease of use. Instead of requiring physical presence for each experimental activity, it will be possible to initiate tests with remote access from Wide Area Network (WAN) or Local Area Network (LAN). This approach will drastically simplify utilization of the test rig in case it is placed in a different room or different geographical location.

b) *Architecture*

In order to accomplish the mentioned requirements in Section 2-a), a complete architecture of the system is proposed in Figure 2. As illustrated, the Cartesian robot is comprised of 4 degrees of freedom with three prismatic joints for motion through Cartesian space and one revolute joint for executing rotational motion in the rotor.

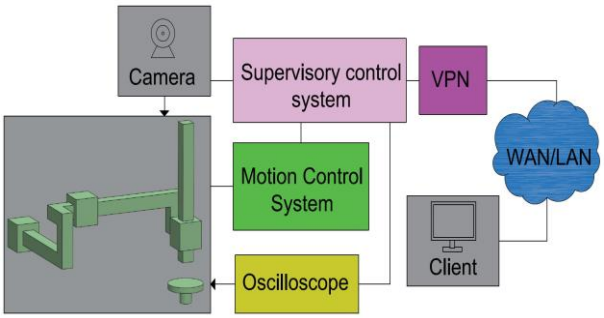


Fig. 2. Test rig architecture

The motion of the robot will be controlled through a dedicated motion control system (MCS) which can be deployed on most widely spread embedded development boards. A supervisory control system (SCS) will communicate with an oscilloscope to initiate measurements. Concurrently the same system will coordinate motion of the robot in between measurements. The SCS will also provide a Graphical User Interface (GUI) for setup and monitoring activities as well as data acquisition in relation to measurements. The same GUI will be accessible through LAN and WAN, allowing for a remote access. For security reasons, access from WAN will only be available through a VPN service. In addition, a camera will be utilized for real time video stream in order to enable visual feedback of the test rig's operation. This SCS can be implemented on any type of computer, however for economic reasons most types of available single-board computers on the market will be suitable for this application.

3. MECHANICAL DESIGN

a) *Linear motion modules*

The prismatic joints of the robot can be realized with linear motion modules, as shown in Figure 3. The structure of the linear module is a 40×80 mm aluminium (Al6060-T5) extrusion profile with T-slots. The T-slots of the profile enable easy and flexible mounting of various components which facilitate greater modularity in the design.

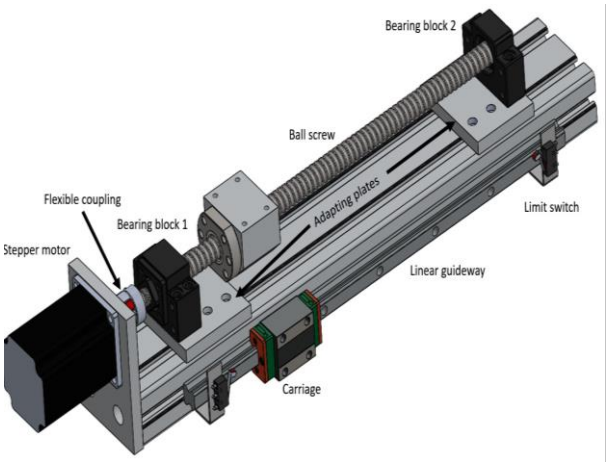


Fig. 3. *X* and *Y* axis linear module

In order to convert rotational motion of a motor into a linear one, a mechanical conversion mechanism is required. Considering the precision requirements of the test rig, a belt driven and ball screw

driven motion were taken into consideration. As shown in Table 1 these two mechanisms demonstrate different properties in regards to precision, speed, backlash, etc. [22]. In the design of this test rig a priority was made on the precision and backlash properties when selecting a linear mechanism. Although belt drives can be very precise in light loads applications, such as in this case, nevertheless a ball screw was considered as a more suitable option.

T a b l e 1

Comparison of ball screws and belt drives

	Ball screws	Belt drives
Thrust	High	Medium
Rigidity	High	Low
Speed	Low	High
Precision	High	Low
Noise	Medium	Medium
Backlash	Low	Medium

The ball screw is mounted on two bearing blocks which are fixated on the T-slots of the extrusion profile. Because the mounting holes of the bearing blocks did not match the T-slots' distance, it was required to add additional custom-made aluminium plates for proper fixation of the bearing blocks. In addition, a linear guideway is utilized in parallel with the ball screw in order to allow for motion and mutual fixture between the axes of the robot.

It was decided that a stepper motor shall be used as a motion actuator, being driven by an open-loop controller. The reason for this choice was because of its low cost and pervasive use in open-source projects. Open-loop stepper motors show disadvantages in motions demanding high accelerations or when driving heavy loads which demand the motor to operate close to its pull-out torque [20]. Such cases may cause the motor to loose steps which will lead to a situation where the controller can not determine its position anymore. The proposed test rig is not intended for driving heavy loads or executing high acceleration motions, therefore stepper motors appeared as a reasonable choice for this application. The motor size can be estimated through calculation of the required torque to drive the ball screw mechanism as [21]:

$$T_u = \frac{FL}{2\pi e} \tag{1}$$

where F is the axial force exerted on the ball screw mechanism in motion, L is the lead of the ball screw and e is its efficiency. This type of module was included in the design for the X and Y axes only. A similar approach was used in the design of Z-axis as well, shown in Figure 4. In order to avoid the full weight of an extrusion profile, like in X and Y axes linear modules, the Z axis' structural components include steel precision rods and custom-made aluminium parts. Since the stepper motor will drive the entire structure of the Z axis, it was crucial that weight reduction was considered in the design.

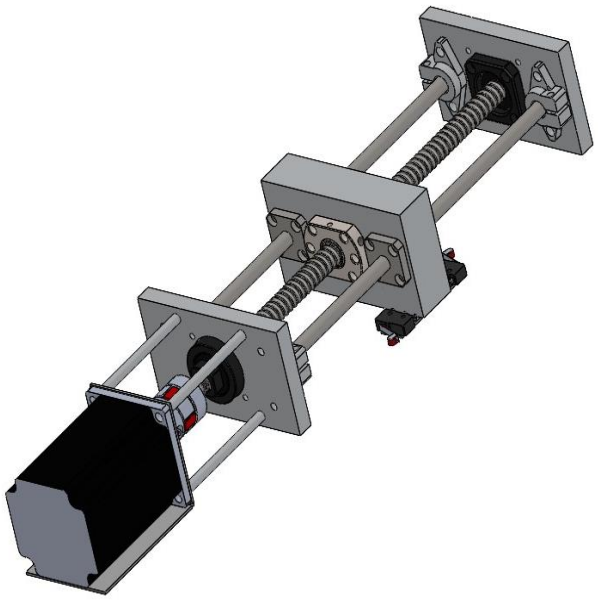


Fig. 4. *Z* axis linear module

b) *Rotary motion module*

In order to achieve a precise rotary motion for the rotor, a motorized rotary indexing table was implemented in the design. The indexing table utilizes a worm gear with high reduction ratio that enables precise rotary motion with high resolution. This indexing table will carry the rotor of the sensor and it is intended to be placed bellow the stator, which will be mounted on the Z axis of the robot. Figure 5 illustrates an example of this indexing table which will be driven by a stepper motor as well. This module will be incorporated as an independent additional axis in the MCS.

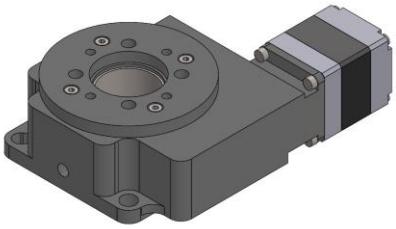


Fig. 5. Rotary indexing table intended for precise rotational motion of the sensor

c) *Robot structure*

The robot structure comprises of combination between 40×40 mm and 40×80 mm aluminium extrusion profiles as shown in Figure 6. The cuboid shape of the entire aluminium structure should provide sufficient rigidity for the robot. In addition, the robot is designed with dual *Y* axis containing two linear modules. Although this approach will potentially introduce the need of synchronization and alignment of the two linear modules, it was considered as a viable solution due to inaccessibility of rigid transmission hardware.

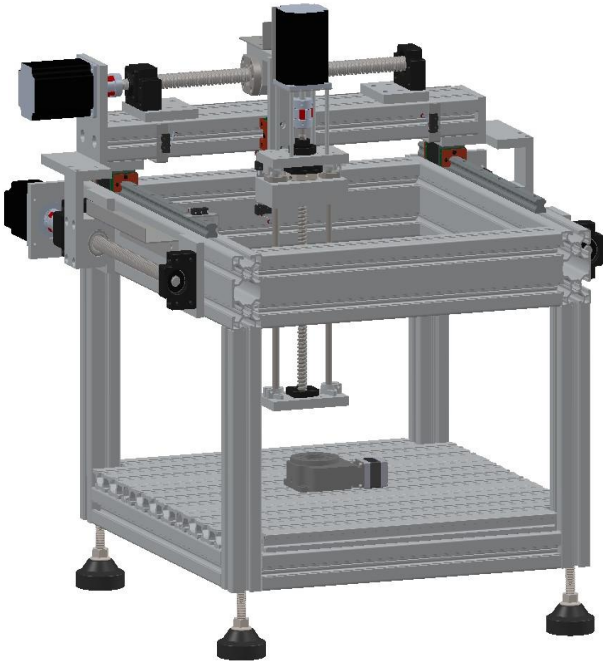


Fig. 6. Complete model of Cartesian robot

For accurate motion of the robot, its gantry should be assembled in a square shape where its dual *Y* axes are almost ideally parallel. For this purpose it is important that the extrusion profiles are precisely cut during procurement. This would allow to utilize *L*-shape connector joints, as shown in Figure 7, which should theoretically enable easy assembly in a precise square shape. This is of course mainly affected by the quality of manufactured *L*-shape connectors. This approach will ensure precise enough assembly and therefore omitting the need for further precision machining. In addition, the connectors shall be mounted in the *T*-slots of the extrusion profiles which will allow for supplementary flexibility and modularity during assembly process. The working table of the robot is comprised of 180×20 mm aluminium extrusion profiles with T-slots, which will ensure easy mounting of additional hardware components.

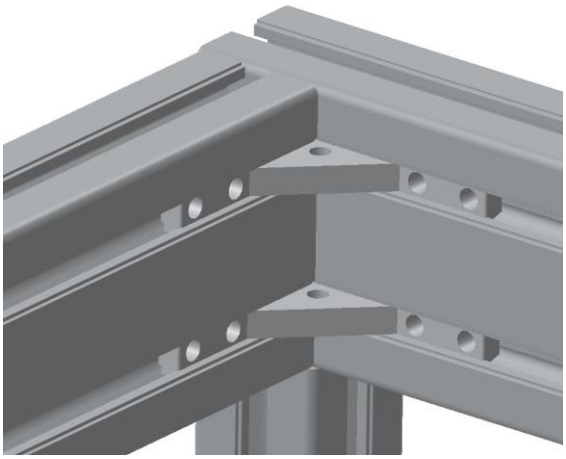


Fig. 7. Connection joints between extrusion profiles

d) *Robot structure*

Considering the decentralized multi-joint control nature of the robot, its forward and inverse kinematics is straightforward and can be easily obtained with the same expression. If it is taken that the reference coordinate system is placed in the origin of *X* and *Y* axes with a distance D_z from the *Z* axis prismatic joint, then the forward kinematics can be expressed as:

$$\begin{cases} x &= d_x \\ y &= d_y \\ z &= D_z - d_z \end{cases} \tag{2}$$

where (d_x, d_y, d_z) is the linear motion of each prismatic. Each linear motion within a linear module is result of converted rotary motion from the motor, which can be expressed as:

$$d = L\frac{\theta}{2\pi} \tag{3}$$

where L is the lead of the ball screw and θ is the rotational position of the motor. Consequently Eq. (2) can be rewritten as:

$$\begin{cases} x &= L_x \frac{\theta_x}{2\pi} \\ y &= L_y \frac{\theta_y}{2\pi} \\ z &= D_z - L_z \frac{\theta_z}{2\pi} \end{cases} \quad (4)$$

where (L_x, L_y, L_z) is the lead of the corresponding ball screw for each linear module and (θ_x, θ_y, θ_z) are the individual rotational positions of the motor.

4. ELECTRICAL AND SOFTWARE DESIGN

The electrical and software design details can be observed in Figure 8. The SCS hosts a web-based GUI software for monitoring and supervisory control activities with the test rig. The client can remotely access the GUI using web communication protocols through LAN or WAN. For security reasons, the remote access from WAN will be intermediated through a VPN service which will be hosted on the SCS. This approach should allow for secure remote connection to the test rig. The client can setup a concrete control strategy for the test rig through the SCS GUI. On the other hand, the SCS executes the control strategy by coordinating the motion of the robot and initiating the process of taking measurements from the oscilloscope. The SCS communicates with the oscilloscope through LAN, using Standard Commands for Programmable Instruments (SCPI), which is a commonly used command set in most commercial oscilloscopes [23]. The test rig can be observed through real time video stream accessed through the SCS software, obtained from a LAN connected camera.

Using USB communication, the MCS will receive the motion commands from the SCS and it will execute them respectively. Each axis stepper motor is driven by an individual motor driver which is controlled from the MCS. In order to achieve synchronized motion, the dual *Y* axis motor drivers will be connected to the same output signals, with the exception of "disable stepper motor" signal. The reason for this is to allow for automatic axis alignment once the axes have been aligned physically. In addition, each axis contains front and back limit switches for homing and protective activities. The *Y* 2-axes limit switches are only added for alignment purposes and therefore can be omitted in alternative design solutions.

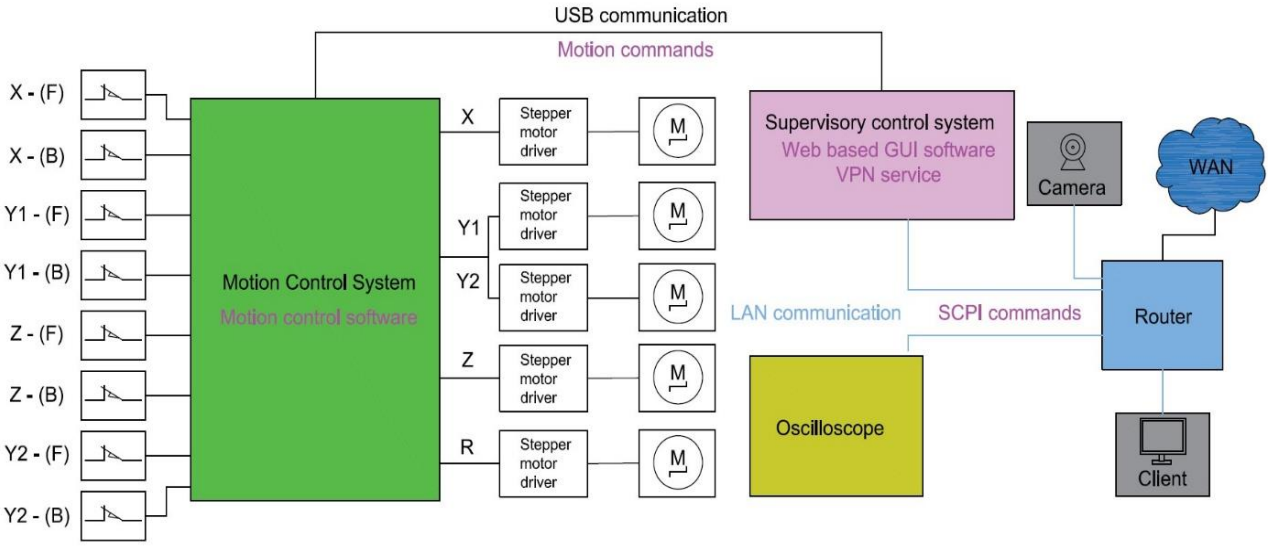


Fig. 8. System architecture with electrical and software details

5. CONCLUSION AND FUTURE WORK

A design solution for a test rig, intended for experimentation with angular position sensors, was proposed. Apart from rotational motion, this configuration allows for performing tests on the sensor through motion in Cartesian space as well. The motion of the robot and measurement triggering is coordinated from a supervisory control system (SCS) running software which allows for setup, monitoring and data acquisition. The SCS software is web-based and therefore allows for remote access

through LAN or WAN which will also stream a real time video from the test rig. The mechanical design of the robot considers a modular and flexible approach in order to allow for easy repurposing of the robot for educational use. Apart from the mechanical design details, in regards to the Cartesian robot, the electrical and software details of the test rig were also shown.

In the future it is intended to perform a practical implementation of the design and test its applicability. The accuracy and repeatability of the robot should be measured in order to establish boundaries of the test rig. Any remarks and possible corrections during mechanical assembly should also be noted. A specific choice in regards to hardware components for the MCS and SCS should be made, along with appropriate software libraries for motion control, VPN service, SCPI communication, etc. A software implementation of the web-based GUI software should be realized along with its communication with the MCS and oscilloscope. Finally a general experimentation test on an angular position sensor should be made in order to establish the usability of the test rig.

REFERENCES

[1] Fleming, W. J. (2001): Overview of automotive sensors, *IEEE Sensors Journa*l, vol. **1**, no. 4, pp. 296–308. doi: 10.1109/7361.983469

[2] Fleming, W. J. (Nov. 2008): New automotive sensors – a review, *IEEE Sensors Journal*, vol. **8**, no. 11, pp. 1900–1921. doi: 10.1109/JSEN.2008.2006452

[3] Reif, K. (ed.) (2015): *Automotive Mechatronics: Automotive Networking, Driving Stability Systems, Electronics*, Springer Vieweg, Wiesbaden, Germany.

[4] Kumar. A. S. A., George, B., Mukhopadhyay, S. C. (2011): Technologies and applications of angle sensors: A review, *IEEE Sens. J*., vol. **21**, no. 6, pp. 7195–7206.

[5] Ebbesson, C. (2011): *Rotary Position Sensors Comparative study of different rotary position sensors for electrical machines used in an hybrid electric vehicle application*, CODEN: LUTEDX/TEIE, Liend University, Sweden.

[6] Datlinger, C., Hirz, M. (2020): Benchmark of rotor position sensor technologies for application in automotive electric drive trains, *Electronics* (Basel), vol. **9**, no. 7, p. 1063.

[7] Simon, M. (2023): *Development of eddy-current rotor position sensor*, Sumida.com. [Online]. [Accessed: 10-Apr-2023], Available: https://www.sumida.com/userfiles/NEWS EVENTS/EVENT SUMMARY/EVTec APE Japan 2014/140523 EVTeC speech.pdf

[8] Janisch, J. (2019): *Inductive Position Sensors, Basic principle.* IDT, A Renesas Company [Online], [Accessed: 10-Apr-2023] Available: https://www.sensor-test.de/assets/de/Aussteller/Ausstel ler-Aktionsprogramm/Fachforen/Manuskripte/JJanisch-IDT-RENESAS.pdf

[9] *Eddy current sensors for automotive and industrial use*. Methodesensor.com,01-Oct-2020. [Online]. Available: https://www.methodesensor.com/technologies/eddy-current-sensors/. [Accessed: 10-Apr-2023].

[10] Brunel, O., Moller, R. (2011): Rotor position sensor for hybrid drives and electric drives new generation eddy current position sensor, *SAE Technical Paper Series*, DOI:10.4271/2011-01-0441.

[11] Wogersien, A., Samson, S., Guttler, J., Beissner, S., Buttgenbach, S. (2004): Novel inductive eddy current sensor for angle measurement, *Proceedings of IEEE Sensors 2003* (IEEE Cat. No. 03CH37498).

[12] *Rotary position sensing for electric vehicles.* Part II. Edn.com. [Online]. Available: https://www.edn.com/ rotary-position-sensing-for-electric-vehicles-part-ii/. [Accessed: 10-Apr-2023].

[13] Sagar, P., Hassan, H. K., Gour, A. S., Karunanithi, R. (2018): Multilayer planar inductor array based angular position sensor for cryogenic application, *Cryogenics* (Guildf.), vol. **96**, pp. 18–24.

[14] Tang, Q., Peng, D., Wu, L., Chen, X. (2015): An inductive angular displacement sensor based on planar coil and contrate rotor, *IEEE Sens. J*., vol. **15**, no. 7, pp. 3947–3954.

[15] Anil Kumar A. S., George, B. (2020): A noncontact angle sensor based on eddy current technique, *IEEE Trans. Instrum. Meas*., vol. **69**, no. 4, pp. 1275–1283.

[16] Straubinger, F., Bartl, J. (2013): *Position encoder and a method for detecting the position of a movable part of a machine*, U.S. Patent 8421446 B2, Apr. 16,.

[17] Ely, D. T. F., Dames, A. N. (2003): *Position sensor having compact arrangement of coils*, U.S. Patent 6522128 B1, Feb. 18.

[18] Lynch, K. M., Park, F. C. (2017): *Modern Robotics : Mechanics, Planning, and Control*. Cambridge, University Press.

[19] Siciliano, B., Khatib, O. (2016): *Springer Handbook of Robotics*. Berlin, Springer.

[20] Hughes, A. (2005): *Electric Motors and Drives : Fundamentals, Types and Aapplications*. Oxford, Newnes.

[21] Mott, R. L., Vavrek, E. M., Wang, Jyhwen (2018): *Machine Elements in Mmechanical Design*. New York, Pearson.

[22] Bosch Rexroth Ag. (2007): *Linear Motion Technology Handbook*. Linear Motion and Assembly Technologies, Schweinfurt, Germany.

[23] Malari, R. (2011): *Instrumentation and Measurement in Electrical Engineering*. Boca Raton, Fla., Brownwalker Press.

[24] Gasparetto, A., Rosati, G. (2002): Design and implementation of a Cartesian robot. In: *AMST'02 Advanced Manufacturing Systems and Technology*, Springer, Vienna, pp. 539–544. http://dx.doi.org/10.1007/978-3-7091-2555-7 61

[25] Hashimdeen, S. H., Miodownik, M., Edirisinghe, M. (2014): The design and construction of an electrohydrodynamic Cartesian robot for the preparation of tissue engineering constructs, *PLOS ONE*, vol. **9**, no. 11, p. e112166. doi: 10.1371/journal.pone.0112166.

[26] McTaggart, M. et al. (2017): *Mechanical Design of a Cartesian Manipulator for Warehouse Pick and Place*, Cornell University, arXiv. doi: 10.48550/arxiv.1710.00967

[27] Bardakas, A., Chasiotis, V. K., Tzempelikos, D., Filios, A. (2014): Design and implementation of a three axis digitally controlled traverse system for flow surveys in a drying chamber, *International Journal of Engineering & Technology*, vol. **3**, no. 3, p. 350. doi:10.14419/ijet.v3i3.3044

Journal of Electrical Engineering and Information Technologies, Vol. **9,** No. 1, pp. 21–31 (2024)
Article 216
Received: November 11, 2023
Accepted: December 30, 2023
In print: ISSN 2545–4250
On line: ISSN 2545–4269
UDC: 621.311.243:004.891.023
https://doi.org/10.51466/JEEIT2491216021sh

Original scientific paper

FORECASTING PV PRODUCTION USING FUZZY REASONING APPROACH

Donard Shaliu, Arlind Çota, Andi Hida, Raimonda Bualoti, Marialis Çelo

Faculty of Electrical Engineering, Polytechnic University of Tirana, Albania
donard.shaliu@gmail.com

A b s t r a c t: In recent years, many studies have been done related to the implementation of methods for PV generation forecasting. The PV generation depends on several factors. Since Artificial Intelligence methods have a greater advantage than other methods, in this paper the construction of a PV energy predictive model of using Fuzzy Logic Approach has been considered. In this paper, a fuzzy reasoning approach is used for prediction of the PV generation. In the proposed method, the fuzzy inferences knowledge-based on IF-THEN rule is developed using MATLAB fuzzy software. Using fuzzy logic, the mathematical representation of influential variables on the prediction of solar power is defined. Three variables influencing the prediction of solar power are taken in consideration as fuzzy logic inputs. These variables are: hours of the day, clouds, tilt angle. The detailed analysis of the fuzzy system surfaces shows that the factors taken in consideration are mutually related. A set of different values of inputs are defined and then PV energy production forecast is made applying the fuzzy approach. The constructed rules based in engineering experience accurately represent forecast of PV generation.

Key words: fuzzy reasoning; influential variables; physical approach; PV generation; statistical approach

ПРОГНОЗА НА ПРОИЗВОДСТВО ОД ФОТОВОЛТАИЧНИ ЦЕНТРАЛИ СО ПРИМЕНА НА ПРИСТАП ЗАСНОВАН НА ФАЗИ РЕЗОНИРАЊЕ

А п с т р а к т: Во текот на последниве години се спроведени голем број истражувања за примена на различни методи за прогноза на производството од фотоволтаичните електрични централи. Производството од овој вид електрични централи зависи од неколку фактори. Земајќи предвид дека методите засновани на вештачка интелигенција имаат предност пред другите методи, во овој труд е прикажан модел за прогноза на производството кој се темели на фази логика. Всушност, со примена на пристапот заснован на фази резонирање се врши прогноза на производството од фотоволтаична електрична централа. Предложениот метод користи фази резонирање засновано на правилото „ако – тогаш“ и е развиен со примена на фази функционалности во програмскиот пакет MATLAB. Користејќи фази логика, се формира математичка репрезентација на величините кои влијаат врз прогнозата на производството од фотоволтаичната централа, а во кои спаѓаат часовите во денот, појавата на облаци и аголот на поставување на модулите. Анализите со примена на фази површини покажуваат дека наведените фактори се заемно зависни. Методот е применет за множество различни влезни величини, при што резултатите покажуваат дека формираните правила кои користат и инженерско искуство можат да дадат точна прогноза на производството од фотоволтаичните централи.

Клучни зборови: фази резонирање; величини кои влијаат на прогнозата; физички пристап; производство од фотоволтаична електрична ценнтрала; статистички пристап

1. INTRODUCTION

The photovoltaic (PV) system generation is an area that is gaining great importance, as the major technology for converting solar energy into electricity, which is reliable, stable and affordable. The effects of the energy crisis that the world experienced since 2021 are still felt, and in the future many challenges are expected. The rise in energy prices and the inflation impact on all energy-consuming sectors shows time dependence to conventional resources. Many countries have realized the

need to focus on solar energy and have undertaken policies that support it via subvention packages. Repower EU is one of the policies created by the European Commission with the aim, among others, to increase the production of renewable energy to 45 % from the current 40 % [1]. Furthermore, the objective is to double the PV installed capacity in the next three years, and the target by 2030 is adding 600 GW PV installed capacities [1]. On the other hand, legal initiatives have also been taken that force constructors to install roof top solar panels for new buildings, commercial and residential ones. Italy is an example where a public program provided financial support, up to 75% of the total capital costs, to install a PV system with peak power between 1 and 20 kWpp [2]. The similar approach has significantly increased the amount of energy produced by rooftop PV panels in many countries [3]. Energy from PV panels has dominated the renewable energy industry for many years. At the end of 2018, the installed on-grid capacity reached a power of 480 GW, i.e., an increase of 20% from the previous year (386 GW). According to IRENA's studies, they show that the production from PV panels can increase to a staggering 2,840 GW capacity globally in 2030 and 8,519 GW in 2050. Globally, 60% of the total capacity will be for mass use and 40% rooftop [4]. As the major technology that converts solar radiation into electricity through PV cells, photovoltaic energy is also reliable, sustainable and affordable for everyone. Many authors see the production of electricity from PVs as a solution for the environmental effects caused by fossil energy sources [5]. Furthermore, it also has positive economic and social effects [6].

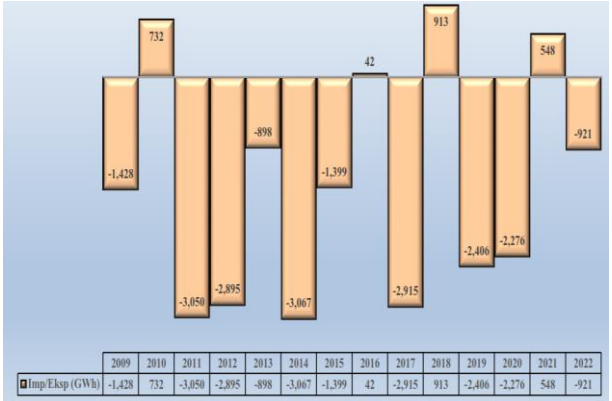
In addition, PV power in Albania is gaining even greater importance because the power system it based on hydro power plant (HPP) production, which depends on yearly hydrologic factors and dry summer periods [7]. On the other hand, the amount of PV generation is affected by various factors such as the tilt angle, irradiation, altitude, temperature, cloudiness, day hours, etc. [8].

Therefore, for the efficient planning and operation of a PV system, accurate forecast of the electricity production is essential. In recent years, many studies have been done for the implementation of methods of forecasting the PV generation. Since Artificial Intelligence methods have a greater advantage than other methods, this paper considers the construction of a PV energy predictive model of using a Fuzzy Logic approach.

The paper is organized as follows: Section 2 provides an overview of Albanian Electrical Power System. PV power forecasting approaches and methods are described in Section 3. Section 4 describes the proposed fuzzy approach. In addition, Section 5 shows the application of the proposed fuzzy approach. The conclusions are provided in Section 6.

2. ALBANIAN POWER SYSTEM OVERVIEW

Albania is a net importer of electricity, as presented in Figure 1 [7], and approximately 100% of the energy is produced by HPPs.



	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Imp/Eksp (GWh)	-1,428	732	-3,050	-2,895	-898	-3,067	-1,399	42	-2,915	913	-2,406	-2,276	548	-921

Fig. 1. Import-export balance of electricity in years 2009–2022 (GWh)

Albania has a great potential of solar energy. Due to its geographical position, the solar irradiation in some areas reaches between 1,185 kWh/m^2 per year to 1,700 kWh/m^2 per year. In optimal meteorological conditions, each square meter can absorb 2200 kWh per year [9].

The total electric production capacity installed until 31st December 2022 is 2,614 MW. Albanian Power Corporation (KESH), a public company, shares 1,448 MW or about 55.4% of the total installed capacity, while the other producers share 1,166 MW or 44.6% of the total installed capacity. The installed capacity of PV is only 23 MWpp or 0.73% of the total capacity [7].

The diversification of electric production capacity is one of the objectives that Albanian government has established in the Strategy of Development of Electric Power System [9]. Albanian policies go in the line with European directives for harmonization of legal framework of energy sector. According to the current policies, small and medium-sized businesses as well as household consumers can install a total capacity of up to 500 KWpp for the production of electricity from renewable sources, such as wind or solar, to cover part or

all of the energy needed and inject the excess into the distribution network [10]. For year 2023, the new PV capacity should increase about 255.2 MWpp [7]. This new scenario of Albanian energy production and the obligation of ALPEX for accurate day-ahead energy forecast require that PV power plants improve their power generation forecasts.

3. PV POWER FORECASTING APPROACHES AND METHODS

Accurate forecasting of PV electricity production is essential for efficient operation and planning of a PV system. The forecasts of PV power output can refer to short terms which include the very short time horizons from few seconds to few minutes, the "intraday" time horizons from 0 to 6 hours ahead, and the day ahead time horizon, which is up to 24 hours ahead. The medium horizon starts from several hours to several days ahead, and the long term begins from several days to several months ahead. The short-term forecasts are used for load control and monitoring in power system operation and in electricity markets [16].

The selection of appropriate forecasting approaches is essential for the forecasting process. In this case, the methods are classified into three approaches: i) the physical approach which is based on the PV power model, ii) the statistical approach which is based on the artificial intelligence and machine learning methods, iii) the hybrid approach, which is based on the mix of the techniques of the same approach or techniques belonging to the other approaches [20].

In physical methods, energy forecasting is based on the use of meteorological parameters (solar radiation and air temperature) predicted by numerical weather prediction (NWP) models. These parameters are used as inputs to a PV system model to forecast the expected power output.

Statistical methods are based on data series measured in the past and are suggested for short time forecasting. In [11] statistical models based on weather data are used. Regression models are discussed in [12]. These models describe the relationship between solar radiation prediction from NWP and PV power production directly from statistical time series analysis from historical data, without considering the physics of the system.

In [13], [14] and [15] statistical models like Artificial Neural Network (ANN) or fuzzy logic are used. ANN is a simple biological analogy of the brain. ANN techniques are based on the neural system and have been widely used to solve PV energy forecasting problems. Fuzzy logic can be interpreted in two different ways. In a narrow perspective it is a logical system. In a broader sense it is synonymous with fuzzy set theory, which refers to communities of objects that have undefined boundaries, and being part of these communities is determined at quantitative levels.

In this paper, fuzzy logic is used in relation to fuzzy set theory. This logic is characterized by the use of linguistic variables, which have words and not numbers as values or parameters. A particularity in the use of fuzzy logic is the use of fuzzy rules. Although words are less precise than numbers, their use is closer to human intuition.

4. PROPOSED FUZZY APPROACH

Fuzzy logic methodology has been in the focus of many researchers which is due to the fact that it operates with a non-linear element [15]. A fuzzy system is characterized by the following elements:

1) input membership function,
2) fuzzy rules, and
3) the output membership function.

The fuzzy reasoning approach involves following steps:

1) Compile the heuristic rules.
2) Perform fuzzy reasoning.

The next step is to decide which inputs will be included in the membership function design and in the fuzzy rules design. We have selected three input variables: hours of the day, cloudiness and the PV module tilt angle. Figure 2 presents the framework of the proposed fuzzy approach.

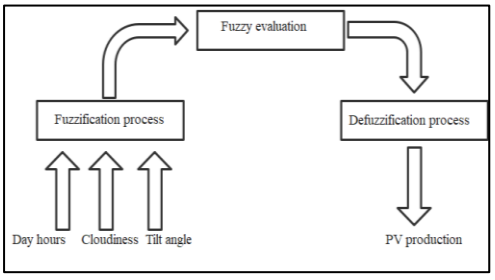


Fig. 2. The framework of the proposed fuzzy approach

a) *Membership functions of input variables*

The input variables are represented by trapezoidal (trapmf) and triangular membership (trimf) function. In the following subsections, the fuzzy model for each variable is presented.

1) Hours of the day

In Figure 3 a typical energy production of PV module during hours of the day [16] is presented. This production is characterized by three parts, the first part is an increase in production, then a constant production, and the third part is a decrease in production [17].

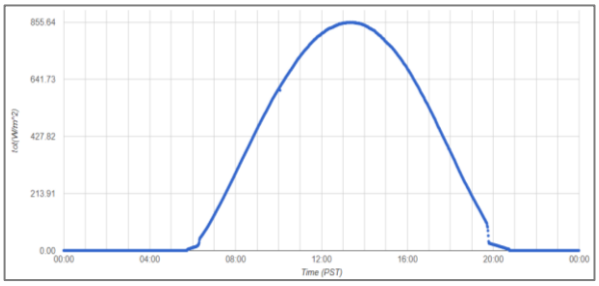


Fig. 3. Typical energy production of PV module during hours of the day

Therefore, the curve can be divided in three sections. Then, the range of each function is defined. Namely, the variable *hours in the day* is designed with three linguistic variables, defined as "AM", which refers to the period between the 7:00 and 10:00, "P" (peak), which is between 9:00 and 15:00 and "PM", which refers to the period between 15:00, and 19:00, as indicated in the Table 1.

T a b l e 1

The linguistic variables of the hours of the day

Linguistic variables	Range
AM	7 – 10
P	8–15
PM	13–19

The membership function for the hours in the day is shown below, in Figure 4. A triangular type (trimf) is selected, and the range of the abscissa values is [7:19], while the range of ordinate values is [0:1]. From Figure 4 it can be observed that the functions interfere.

2) Cloudiness

The numerical values of the *cloudiness* inputs are divided into groups named "Low" (slightly cloudy), "MC" (moderately cloudy), "VC" (very cloudy) and "TC" (totally cloudy), as indicated in the Table 2.

T a b l e 2

The linguistic variables of the cloudiness

Linguistic variables	Range
Low	–36 – 30
MC	15 – 50
VC	40 – 80
TC	70 –145

After determining the range of function on the abscissa axis, we build the membership functions of the cloudiness input in the interval fuzzy system. All four membership functions extend to the interval [0:1] on the ordinate axis, while on the abscissa axis to the interval [0:100]. From Figure. 4 it could be noticed that the functions interfere between one another and in addition to the triangular type, the trapezoidal type (trapmf) is also used. The Figure 5 shows the membership functions of the cloudiness input.

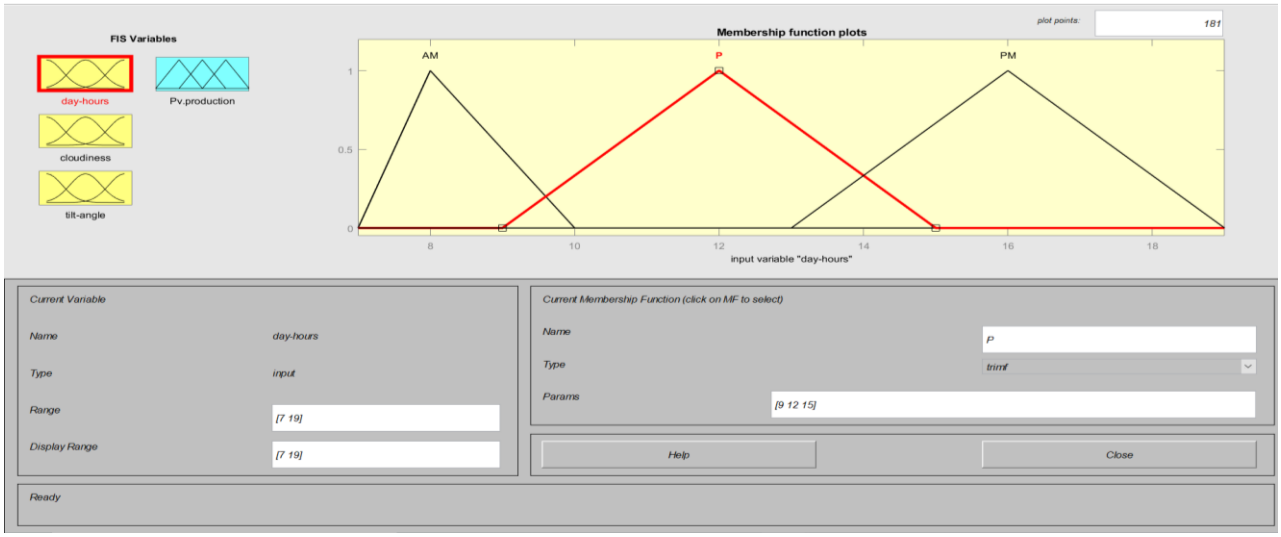


Fig. 4. Membership functions indicator for the hours in the day input

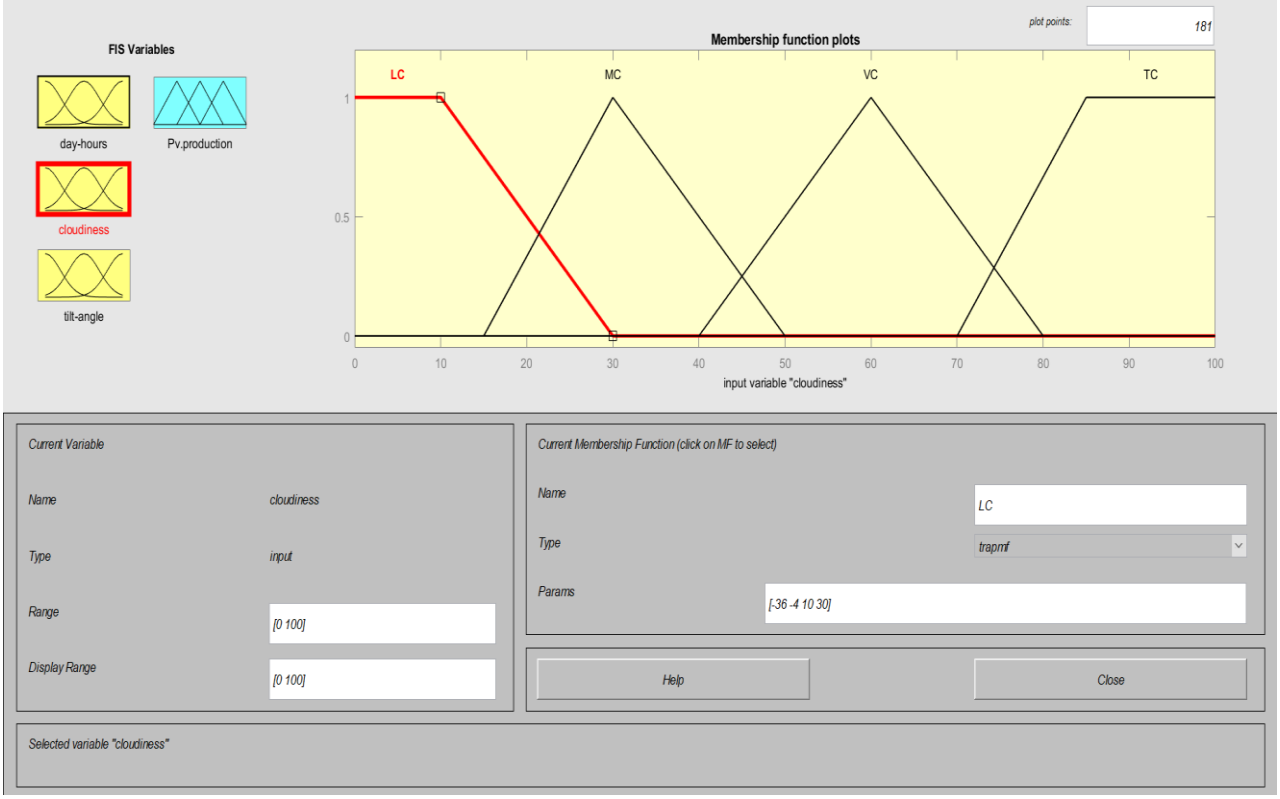


Fig. 5. Membership functions indicator for the cloudiness input

3) Tilt angle

The *tilt angle* and orientation of the panels are determining factors in the production of photovoltaic panels [5, 18]. In Figure 6 the dependency of the PV energy production from the tilt angle is presented [19]. We have referred to this graph as a model to help us determine the intervals of the tilt angle variables in the fuzzy system in Matlab.

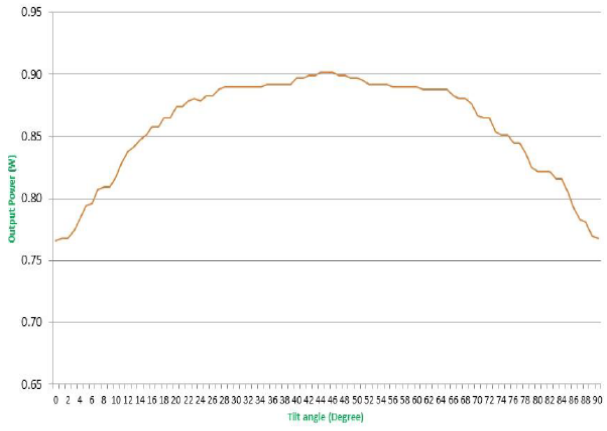


Fig. 6. Graph of the PV power output panel as a function of the tilt angle

The numeric values of the tilt angle input are divided into three units, i.e., "H" (horizontal), "Az" (azimuth angle, optimal), "V" (vertical), and the limits of each interval have been determined. The intervals belonging to each community are shown in the Table 3.

T a b l e 3

The linguistic variables of the tilt angle

Linguistic variables	Range
H	–36 – 30
Az	15 – 50
V	40 – 80

Once the range of each function on the abscissa axis is determined, the membership functions of the inputs to the fuzzy system are constructed. Figure 7 shows the membership functions of the input tilt angle. When a numerical value of the input tilt angle is written to the system, the system automatically defines which function the numerical value belongs to. As mentioned before, the tilt angle input contains the three membership functions, i.e. "H", "Az", and "V". The extent limits in 2-dimensional space are defined in the white field labelled "Params". In the "Type" section, the triangular type (trimf) is selected. The interval of abscissa values is 0:90, while the interval of ordinate values is 0:1.

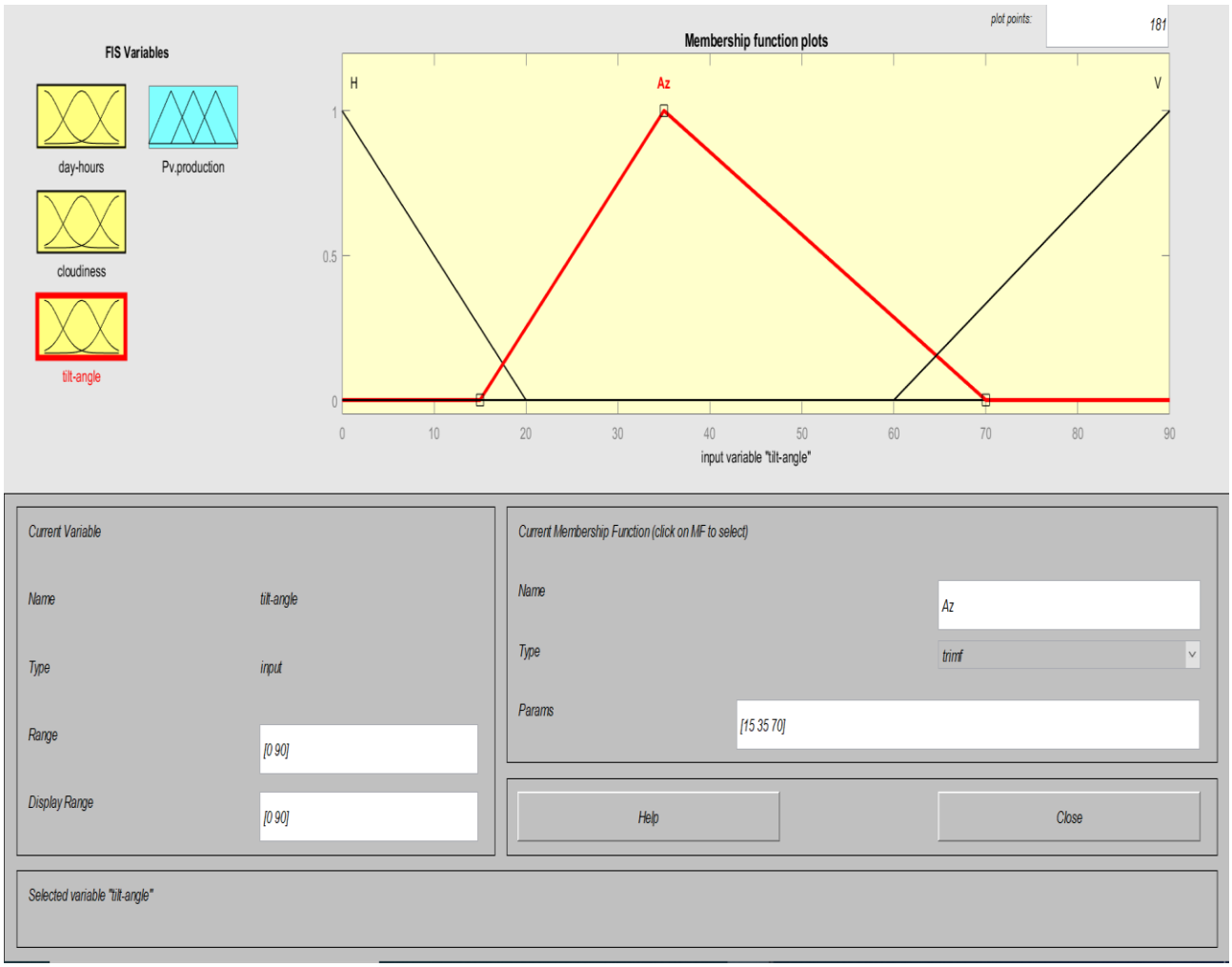


Fig. 7. Membershi functions indicator tilt angle input

From the Figure 7 it could also be observed that the functions interfere with one another.

b) *Output fuzzy membership function*

The *PV production* is used as an output variable. PV production is designed with four linguistic variables defined as "Zero" (zero production), "LP" (low production), "MP" (medium production), "HP" (high production). We first defined the range of each function as indicated in the Table 4.

After defining the range of function on the abscissa axis, we build the membership functions of the output *PV production*, as shown in Figure 8 below.

The output *PV production* contains the four membership functions, i.e. "Zero", "LP", "MP", and "HP". The selected membership function type is triangular. The base of each triangle is extended into 2 units. The selected function MP has its base in the interval [20, 70], while the third peak is in the *x-y* coordinates (5, 1). All four membership functions extend to the interval [0:1] on the ordinate axis, while on the abscissa axis to the interval [0:100]. As presented in Figure 8 the functions interfere with one another and in addition to the triangular type, the trapezoidal type (trapmf) is also used.

T a b l e 4

The linguistic variables of PV production

Linguistic variables	Range
Zero	0 – 10
LP	10 – 30
MP	20 – 70
HP	60 –140

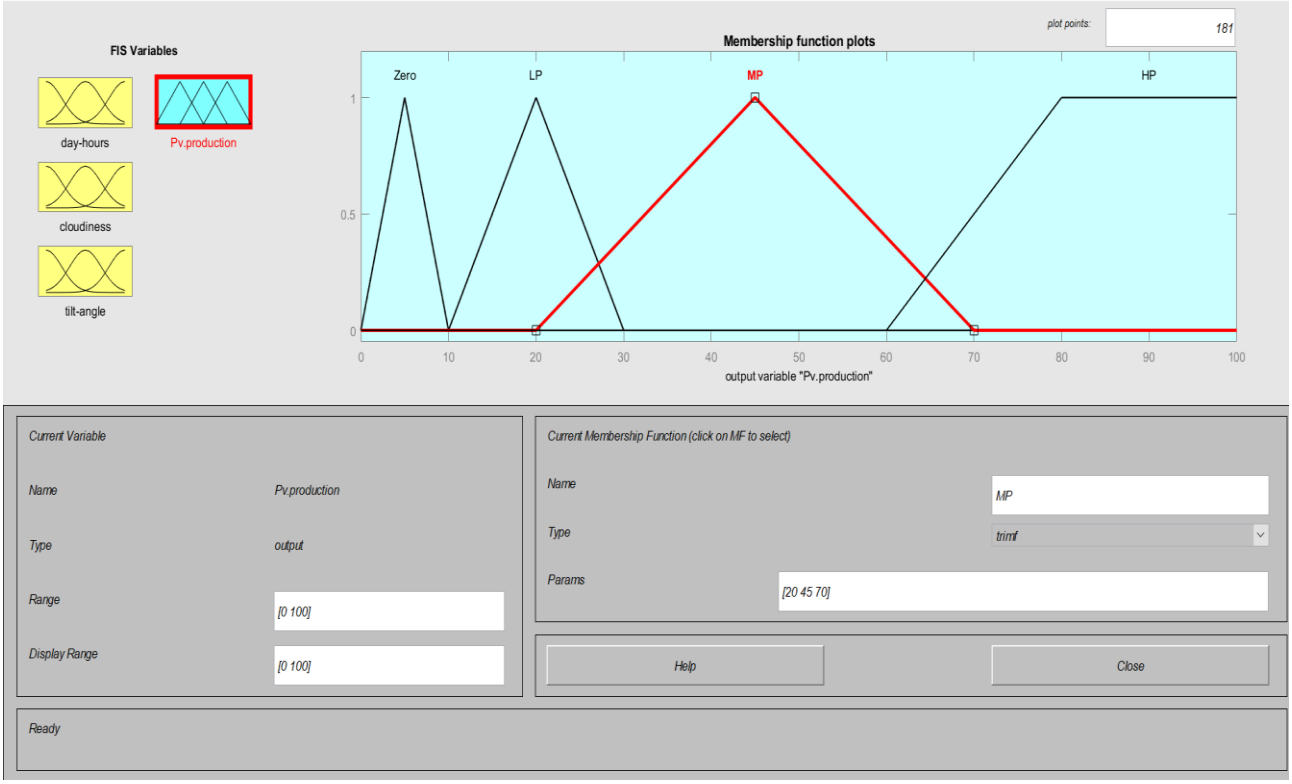


Fig. 8. Membership functions indicator PV production output

5. APPLICATION OF THE PROPOSED FUZZY APPROACH

In the proposed method, a fuzzy knowledge-based approach is developed. To evaluate the PV energy production, the Fuzzy Inference System (FIS) editor of MATLAB Fuzzy Logic Toolbox is used. The component relations of the fuzzy system are shown in the Figure 9. In the last step of the methodology, the fuzzy logic toolbox of MATLAB was applied for introducing the membership functions and the fuzzy rules. Furthermore, the software helped to automate the evaluation of the PV production.

a) *Fuzzy inference rules*

To define the fuzzy inference rules the following steps are taken:

1) Define the total numbers of interactions between the input output variables.

2) The output for each rule was determined by the references and practical experience.

Each rule consists of two components which are the antecedent (IF part) and the consequent (THEN part). With the fuzzy logic technique, partial output membership can be improved by increasing the number of rules. In the process of fuzzy approach, we have used the Centroid methods.

For the fuzzy logic control, Mamdani's Max-Min composition technique is used. FIS derives output fuzzy sets from judging all the fuzzy rules by finding the weighted average of all 26 fuzzy rules. Using the Fuzzy Rule Viewer, the impact of each input on the output production value can be observed, as shown in Figure 10.

Four cases are considered to determine the influence of each input on the output, where one of the inputs receives four different values, while the other two are kept unchanged. The same process is repeated for each input variable.

From Figure 11 the influence of the input value hours of the day on the value of the output is observed, keeping the other two inputs constant. For different values for the input variable hours of the day (8, 12, 14, 16) we notice that the values of the output increase. Also, it is worth saying that during peak (P) and afternoon (PM) we get higher values of PV production.

From Figure 12, the impact of the increase in the percentage of clouds on the output PV production can be observed. Keeping constant values of the other two input variables, the PV production is decreasing. The less clouds we have, the higher the production will be.

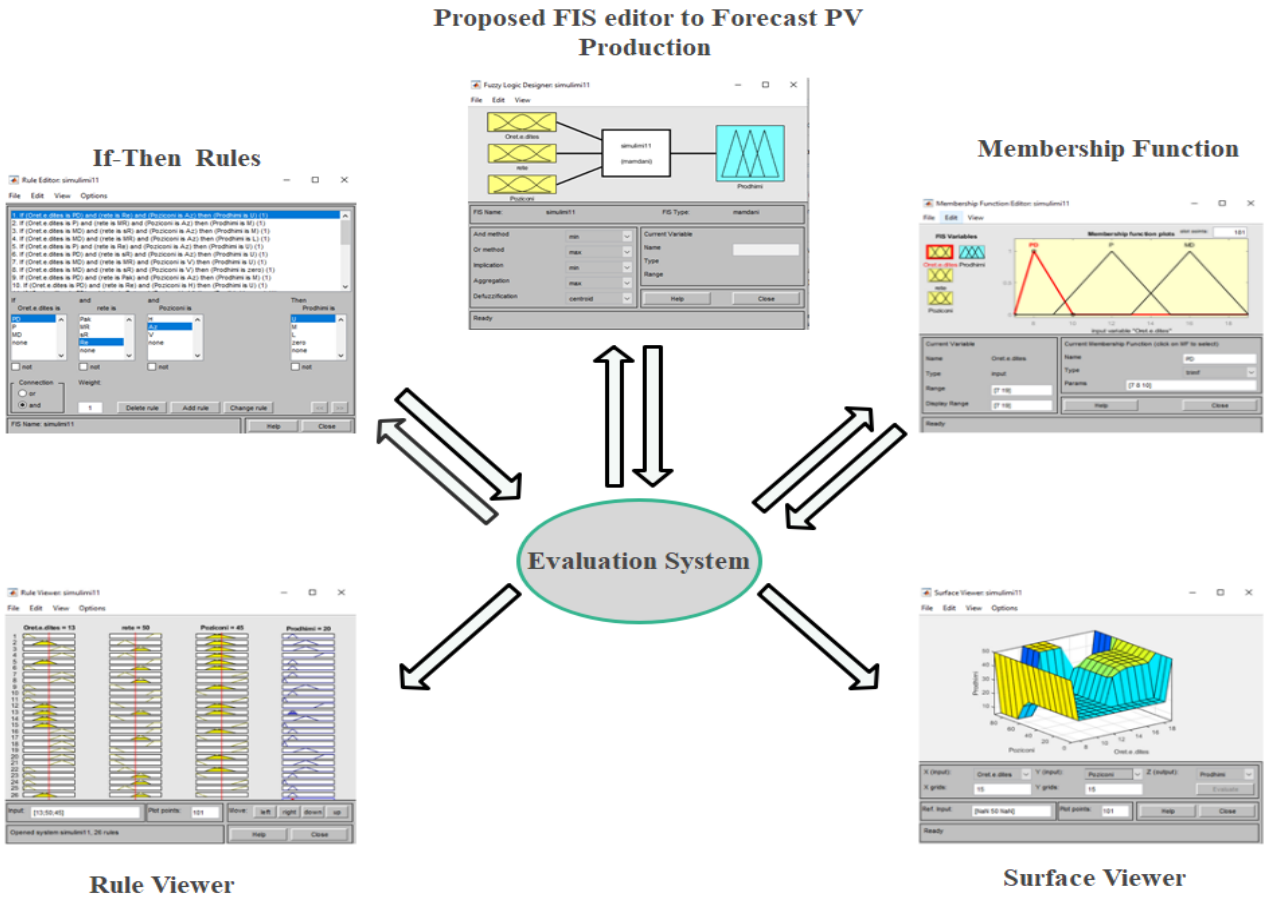


Fig. 9. Interaction of system tools with each other

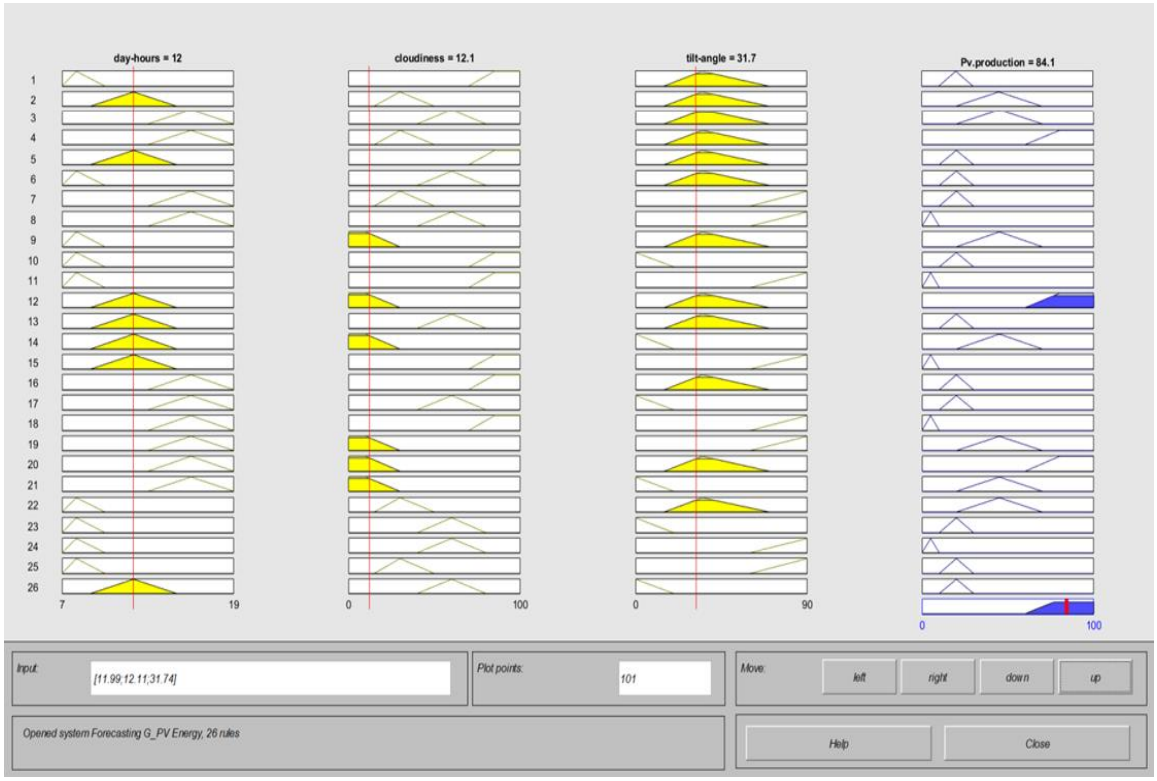


Fig. 10. The impact of each input on the output value

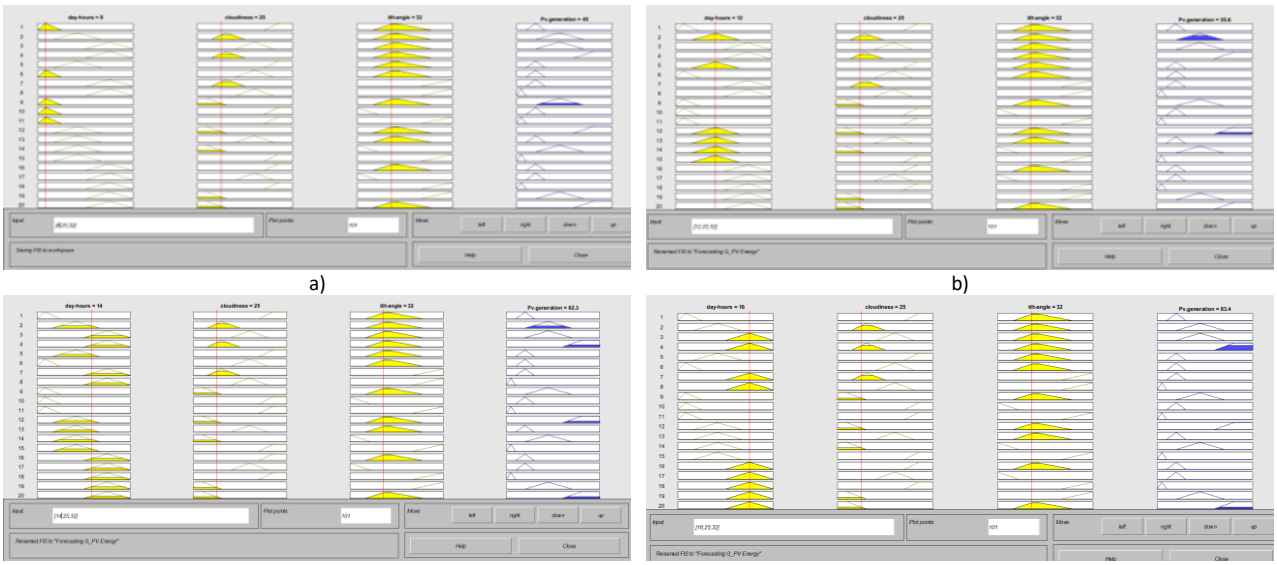


Fig. 11. The influence of the input hours of the day on the value of the output PV production on fuzzy inference rules a) "hour of the day" is 8 and all other inputs are constant; b) "hour of the day" is 12 and all other inputs are constant, c) "hour of the day" is 14 and all other inputs are constant; d) "hour of the day" is 16 and all other inputs are constant

Fig. 12. Fuzzy inference rules, the influence of the input cloudiness on the output PV production value

In the same way we changed the values of the tilt angle variable, it can be observed that for positioning of the PV panel at the optimal angle Az, the PV production is higher than in the horizontal or vertical positioning. When comparing the horizontal and vertical position of the panel, there is only a slight difference of the output.

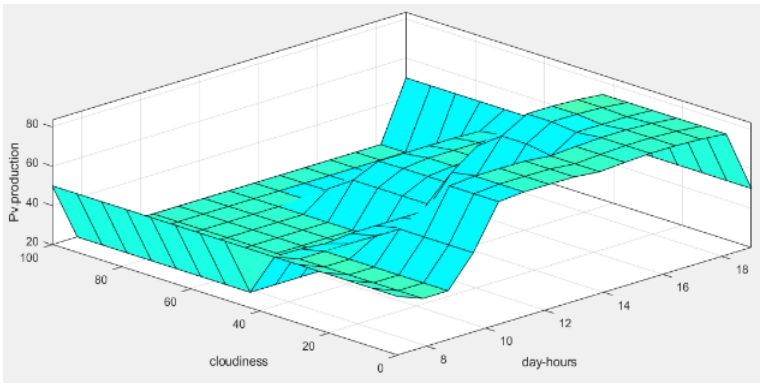
Table 5 provides comparison of the output value of the fuzzy approach with linguistic output variable. It can be observed that the same result is obtained with the value defined by the fuzzy approach and fuzzy output variable.

Figure 13 shows the effect of combination of two inputs on the output value (production), while setting one input constant.

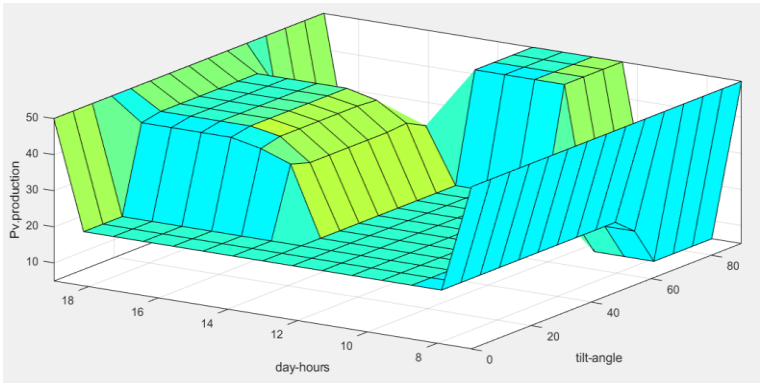
T a b l e 5

Comparison of the fuzzy approach output value and the linguistic output variable

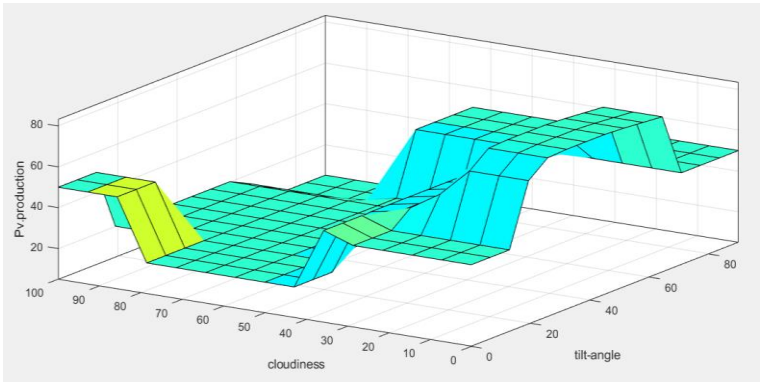
Nr.	Inputs			Output	
	Day hours	Cloudiness (%)	Tilt angle (˚)	Production (%)	
1.	8	15	30	45	MP
2.	12	15	30	83.7	HP
3.	8	75	30	20	LP
4.	12	75	30	20	LP
5.	8	15	70	50	MP
6.	12	15	70	50	MP
7.	8	75	70	5	zero
8.	12	75	70	5	zero



a)



b)



c)

Fig. 13. The influence of different factors to the PV production:
a) influence of cloudiness and day hours, b) influence of day hours and tilt angle,
c) influence of cloudiness and tilt angle

6. CONCLUSION

In this paper a fuzzy approach is presented for PV production forecast, taking in to account the day hours, weather conditions and tilt angle.

From the obtained results it can be observed that different combination of input values should be taken into account to define the final result. Fuzzy approach gives us the possibility to take into account these combinations.

Furthermore, this method permits to use the engineering experience and data sets in defining fuzzy rules, enables the interpretation of the different factors that affect the PV production, turning them into logical conditions.

The proposed fuzzy approach gives satisfactory results for the prediction of energy production from photovoltaic. Moreover, helps in the correct decision-making and risk management of the producers that participate in the electricity market timeframes, avoiding penalties.

REFERENCES

[1] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_3131

[2] Song, A., Lu, L., Liu, Z., Wong, M. S. (2016): A study of incentive policies for building-integrated photovoltaic technology in Hong Kong. *Sustainability* **8** (8), 769. https://doi.org/10.3390/su8080769

[3] Kılıç. U, Kekezoğlu, B. (2022): A review of solar photovoltaic incentives and policy: Selected countries and Turkey. *Ain Shams Engineering Journal*, Volume **13**, Issue 5, 101669. https://doi.org/10.1016/j.asej.2021.101669

[4] IRENA (2019), *Global Energy Transformation: A Roadmap to 2050*, International Renewable Energy Agency, Abu Dhabi. ISBN: 978-92-9260-121-8

[5] Hamed, T. A., Alshare, A. (2021): Environmental impact of solar and wind energy – a review, *J. Sustain. Dev. Energy Water Environ. Syst.* Vol. **10**, Iss. 2, 1090387. DOI: http://dx.doi.org/10.13044/j.sdewes.d9.0387

[6] Changsheng Li, Haiyu Wang, Hong Miao, Bin Ye (2017): The economic and social performance of integrated photovoltaic and agricultural greenhouses systems: Case study in China, *Applied Energy*, Vol. **190**, pp. 204–212. https://doi.org/10.1016/j.apenergy.2016.12.121

[7] https://www.ere.gov.al/en/publications/annual-reports

[8] Hida, A., Kërçi, T., Bualoti, R., Çelo, M., Shaliu, D. (2022): A techno-economic analysis of a photovoltaic plant: an Albanian case study, *International Conference on Renewable Energies and Smart Technologies (REST)*, Tirana, Albania, pp. 1–5. DOI: 10.1109/REST54687.2022.10022337

[9] http://www.akbn.gov.al/wp-content/uploads/2019/05/Renewable-Energy.pdf

[10] https://kpmg.com/al/en/home/insights/2023/05/new-law-on--promotion-of-the-use-of-energy-from-renewable-source.html

[11] De Giorgi, M. G., Congedo, P. M., Malvoni, M. (2014): Photovoltaic power forecasting using statistical methods: impact of weather data. *IET Sci. Meas. Technol*., **8**, pp. 90–97. https://doi.org/10.1049/iet-smt.2013.0135

[12] Karamdel, S., Liang, X., Faried, S. O., Shabbir, M. N. S. K. (2022): A Regression model-based short-term pv power generation forecasting, *IEEE Electrical Power and Energy Conference (EPEC)*, Victoria, BC, Canada, pp. 261–266, DOI: 10.1109/EPEC56903.2022.10000086.

[13] Abuella, M., Chowdhury, B. (2015): Solar power forecasting using artificial neural networks, *North American Power Symposium (NAPS)*, Charlotte, NC, USA, pp. 1–5. DOI: 10.1109/NAPS.2015.7335176.

[14] Ncane, Z. P., Saha, A. K. (2019): Forecasting solar power generation using fuzzy logic and artificial neural network, *2019 Southern African Universities Power Engineering Conference/Robotics and Mechatronics / Pattern Recognition Association of South Africa (SAUPEC / Rob Mech/ PRASA)*, Bloemfontein, South Africa, pp. 518–523, DOI: 10.1109/RoboMech.2019.8704737

[15] Tabish Ansari, M., Rizwan, M. (2022): Solar energy forecasting using fuzzy logic and artificial neural network. In: Palani, I. A., Sathiya, P., Palanisamy, D. (eds): *Recent Advances in Materials and Modern Manufacturing. Lecture Notes in Mechanical Engineering*. Springer, Singapore. https://doi.org/10.1007/978-981-19-0244-4_47

[16] Li. Z., Rahman, S., Vega, R., Dong, B. (2016): A hierarchical approach using machine learning methods in solar photovoltaic energy production forecasting, *Energies*, vol. **9**, no. 1, p. 55. https://doi.org/10.3390/en9010055

[17] Casula, L., D'Amico, G., Masala, G. et al. (2020): Performance estimation of photovoltaic energy production. *Lett Spat Resour Sci* **13**, 267–285. https://doi.org/10.1007/s12076-020-00258-x

[18] Yunus Khan, T. M., Soudagar, M. E. M., Kanchan, M. et al. (2020): Optimum location and influence of tilt angle on performance of solar PV panels. *J Therm Anal Calorim* **141**, 511–532. https://doi.org/10.1007/s10973-019-09089-5

[19] Shareef, M. (2017): The impact of tilt angle on photovoltaic panel output. *ZANCO Journal of Pure and Applied Sciences* **29** (15), 112–118. DOI: 10.21271/ZJPAS.29.5.12

[20] Abdelhakim El Hendouzi, Abdennaser Bourouhou (2020): Solar photovoltaic power forecasting, *Journal of Electrical and Computer Engineering*, vol. **2020**, iss. 1, Article ID 8819925, p. 21. https://doi.org/10.1155/2020/8819925

Journal of Electrical Engineering and Information Technologies, Vol. **9,** No. 1, pp. 33–41 (2024)
Article 217
Received: November 16, 2023
Accepted: December 25, 2023
In print: ISSN 2545–4250
On line: ISSN 2545–4269
UDC: 621.395.721.5:004.77]:[004.8:620.92-027.236
https://doi.org/10.51466/JEEIT2491217033k

Original scientific paper

ENERGY EFFICIENCY IN 6G MOBILE NETWORKS

Stojan Kitanov[1], Ivan Petrov[2], Vladimir Nikolić[3], Toni Janevski[4]
[1]*Mother Teresa University, Faculty of Informatics, Skopje, N. Macedonia*
[2]*School of Computer Science and Information Technology, University American College, Skopje, N. Macedonia*
[3]*European University, Faculty of Informatics, Skopje, N. Macedonia*
[4]*Faculty of Electrical Engineering and Information Technologies, Ss. Cyril and Methodius University in Skopje, N. Macedonia,*
stojan.kitanov@unt.edu.mk

A b s t r a c t: The 5G network technology is finding its use in variety of sectors in the global industry. Significant improvements are achieved in terms of latency, data rates, spectral efficiency, mobility, and number of connected smart mobile devices. Digital society and smart cities are reality. 5G networks offer a wide range of applications and services, but still have some limitations regarding the rapidly increasing data traffic demands. The focus of the research and development activities are set on the next 6G mobile and wireless networks, which are expected to be commercially available around 2030. In this direction, this paper proposes a 6G Advanced Wireless Mobile Heterogeneous Access Network (6G AWN-HAN) architecture with artificial intelligence, whose description is expected to contribute in defining the specification standards of 6G network. It also evaluates the performance quality of artificially intelligently, orchestrated services in 6G mobile networks in terms of energy efficiency. The research results show a significant improvement in energy efficiency by applying artificial intelligence at the edge of the network.

Key words: 5G; 6G; artificial intelligence; Internet of Things

ЕНЕРГЕТСКА ЕФИКАСНОСТ ВО МОБИЛНИ 6G-МРЕЖИ

А п с т р а к т: Мрежната 5G технологија ја наоѓа својата примена во различни сектори од глобалната индустрија. Постигнати се значителни подобрувања во однос на латентноста, брзините на пренос на податоци, спектралната ефикасност, мобилноста и бројот на поврзани мобилни уреди. Дигиталното општество и паметните градови се реалност. 5G-мрежите нудат широк опсег на апликации и услуги, но сепак имаат одредени ограничувања во однос на рапидното зголемување на барањата за сообраќај на податоци. Фокусот на активностите за истражување и развој е поставен на следните мобилни 6G-мрежи, кои се очекува да бидат комерцијално достапни околу 2030 година. Во таа насока, овој труд предлага архитектура на напредна безжична мобилна хетерогена пристапна 6G-мрежа (6G AWN-HAN) со вештачка интелигенција, чиј опис се очекува да придонесе за дефинирањето на спецификациите на стандардот за 6G-мрежата. Исто така се евалуира квалитетот на перформансите на вештачки интелигентно оркестрирани услуги во мобилните 6G-мрежи во смисла на енергетската ефикасност. Резултатите од истражувањето покажуваат значително подобрување на енергетската ефикасност со примена на вештачката интелегенција на работ од мрежата.

Клучни зборови: 5G; 6G; вештачка интелигенција, интернет на нештата

1. INTRODUCTION

5G mobile and wireless networks achieved significant improvements in terms of latency, data rates, spectral efficiency, mobility, and number of connected smart mobile devices. Therefore, they have marked the beginning of a true digital society.

Nowadays there is a shift towards a society of fully automated and remote management systems in number of business sectors and industries. The rapid development of artificial intelligence (AI), virtual

reality, three-dimensional (3D) media, and the Internet of Everything (IoE), has led to a massive volume of traffic [1]. The global mobile traffic in 2030 is predicted to be around 5000 EB/month [2].

However, up to the present moment, 5G mobile communications have so far provided little added value for consumers due to the high cost of the services, and inadequate availability (especially in rural areas). In addition, 5G requires more transmission antennas for uniform network coverage than 4G network.

Although 5G network offers support of many broadband applications and services, still it may not be able to meet the rapid increase of the traffic demands [3]. In particular, the holographic communication may require a data rate up to terabits per second (Tb/s), that is almost three times higher than the 5G's data rate and massive low latency (hundreds of microseconds), which is three time less than 5G's latency [4 – 6]. Moreover, because of the ever-increasing growth of the deployment of Internet of Things (IoT) and future Internet of Everything (IoE) devices, it would be necessary to improve further the connection density and coverage of 5G enabled IoT networks [7 – 8]. In addition, the future mobile networks are expected to be ultra-large-scale, highly dynamic, and incredibly complex system. Therefore, the manual optimization and configuration tasks used in the existing mobile networks would be no longer suitable for the next generation mobile networks [9 – 12]. At last, the new emerging services of Internet of Everything (IoE) such as extended reality (XR), telemedicine systems, mind-machine interface (MMI), and autonomous cars would demand high transmission rates, high reliability, and low latency, which significantly exceeds the original goals of the 5G networks [13 – 15].

Therefore, after the global deployment as well as global commercialization of 5G mobile network, the 6G network research initiatives have gained significant attention in both academy and industry.

The main goal of 6G network is communication at any time, and at any place with delay of 1 microsecond, and high data rate speed, by using higher-bandwidth frequencies over the longer distances than 5G network, such as THz waves, and artificial intelligence (AI). Due to the proliferation of IoT devices, the next generation of communication systems must meet stringent requirements for spectrum and energy economy, low latency and high throughput. These IoT devices would pave the way for novel services like telemedicine, virtual reality (VR) and extended reality (XR), environment-tal telemetry and condition tracking, autonomous cars, and linked drones and robots capable of transmitting full]HD video.

Artificial intelligence (AI) will be the main driving force in designing and optimizing 6G architectures, protocols, and operations. These networks would drastically re-shape the wireless evolution from "connected things" to "connected intelligence" [16]. 6G would provide support of ubiquitous and mobiquitous AI services from the core to the end devices of the network, which would exceed the mobile internet used today.

Now the initiatives of 6G primarily focus on identifying the main drivers, performance requirements, and technological innovations related to 6G.

In this direction, this paper highlights the vision of the technologies used in 6G network, 6G network scenario, 6G network challenges and potential solutions. The main contribution of this paper is the proposal of a 6G Advanced Wireless Mobile Heterogeneous Access Network (6G AWN-HAN) Architecture with artificial intelligence, whose description is expected to define the standard of 6G network.

Furthermore, it evaluates the performance quality of artificially intelligently, orchestrated services in 6G mobile networks in terms of energy efficiency. For this purpose it is used an analytical model where energy efficiency is expressed as the amount of user data rate transmission per user power consumption. The user data rate transmission, i.e., user throughput represents the quantity of data that can pass from source to destination in a specific time. In the simplest way it can be equal to the peak data rate equally shared by the users. For simplicity the user power consumption is expressed as a linear function of the user throughput. The research results show a significant improvement in energy efficiency by applying artificial intelligence at the edge of the network.

The rest of the paper is organized as follows. Section 2 explains the roadmap of 6G network. Section 3 provides details about 6G network requirements. Advanced AI 6G network model is evaluated in Section 4. Section 5 proposes 6G network architecture. Section 6 provides details of energy efficiency in 6G network and section 7 concludes the paper, addresses the challenges in 6G network that need to be resolved and provides directions for future work.

2. THE ROADMAP TO 6G NETWORK

Different standard organizations and bodies have proposed different roadmaps of 6G network [16]. The roadmap of 6G network envisioned by different organization standards, such as 3GPP, ITU, and PoC, is presented in Figure 1.

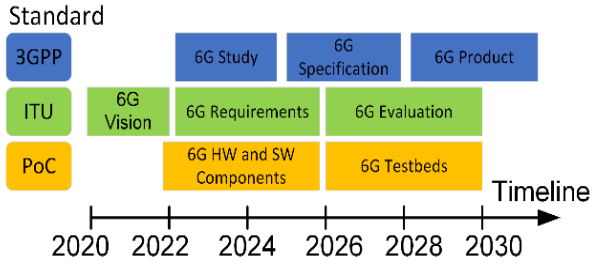


Fig. 1. The roadmap of 6G network

The phase about the vision of 6G network is already completed at the beginning of 2022. The next phase that includes study and definition of the 6G network requirements, as well as development of 6G network components has started in 2022. The definition of specification and standards of 6G network are expected to start around 2025. The evaluation and the testbeds of 6G network are expected to begin in 2026. The first 6G commercially deployed network would be after 2030.

3. 6G NETWORK REQUIREMENTS

6G mobile and wireless networks is expected to provide large coverage that allows subscribers to communicate with one another everywhere with a high data rate speed. To address the challenges and the issues that 5G network currently faces, it is necessary 6G network to be developed, innovative operations in shared spectrum bands among the network operators to be implemented, cooperation strategies in heterogeneous networks, and leasing networking slices on-demand to be used. In addition, 6G network would require higher frequency bands in the terahertz spectrum, quite large and opportunistic data rate to support demanding multimedia applications [17]. The end-to-end delay in 6G network should be less than 1 millisecond (about 1 μs), in order augmented reality, telepresence, and other delay sensitive services to be supported. Furthermore, 6G network should provide improved reliability comparing to 5G, in order mission and safety-critical applications to be enabled.

A comparison between 5G and 6G network parameters and requirements is given in [18, 19]. All parameters such as traffic capacity, data rate, end-to-end delay, processing delay, spectral and energy efficiency, etc. are expected to be improved several times over the value provided by 5G. A comparison between 5G and of 6G parameters are given in Table 1.

T a b l e 1

A comparison of KPI requirements between 5G and 6G network

Parameter requirement	5G	6G
End-to-end delay	1 ms	1 μs
Traffic capacity	10 Mbit/s/m^2	10 Gbit/s/m^3
Latency	Fair	Slightly annoying
Localization precision	10 cm on 2D space	1 cm on 3D space
User experience	50 Mbit/s everywhere on 2D space	10 Gbit/s everywhere on 3D space
Downlink peak data rate	100 Gbit/s	1 Tbit/s
Uplink peak data rate	50 Gbit/s	~ 1 Tbit/s
Frame error rate (FER) reliability	10–5	10–9
Spectral and energy efficiency compared to today's network	10 up to 100 times in bits/s/Hz/m2/J	1000 times in bits/s/Hz/m^3/J (volumetric)

6G network would provide new use cases, which cannot be completely supported by 5G [19]. Some of them are holographic telepresence, industrial automation (industry 4.0 transform), e-health, tactile internet, augmented, and virtual reality.

As a result, many 6G services would appear. Most of the 6G services would be a hybrid combination of several 5G services. The services in 6G network would require low latency, high reliability, high data rate, massive connectivity, and full mobility. Some of the possible 6G services are massive URLLC (mURLLC), enhanced mobile broadband URLLC (eURLLC), and massive eMBB (meMBB) [19].

4. ADVANCED AI NETWORK MODEL FOR 6G

6G network would not be able to provide the necessary complex services demanded by the users

with the guaranteed QoS and QoE parameters only by involvement of the humans in performing the manual network configuration and optimization. This can be achieved only by support of artificial intelligence (AI), which will auto-reconfigure and auto-optimize the network quickly enough to maximize traffic routing in order spectral efficiency to meet the service requirements. AI represents the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic for humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.

Therefore, AI is the most influential and recently proposed enabling technology for the 6G network [20]. The conventional approach is to place the AI in the 6G core in all TCP/IP layers. This would introduce descriptive, diagnostic, predictive and prescriptive AI data analytics that will analyze the collected historical data to get insights of the network status especially of the PHY, MAC, Network and Transport layer [20, 21].

However, if the AI is placed only in the core part of the network, 6G would not be able to deal with the future Internet services and applications. This is because the conventional AI core service orchestration approaches that have been applied are not adequate to deal with the forthcoming large-scale and dynamic services and applications, since they cannot effectively cope with reduced latency, high mobility, high scalability, and real-time execution.

Therefore, another promising computing paradigm that recently started to gain enormous interest is the edge intelligence (EI) or edge AI located at the edge of the network [22, 23]. Moreover, big data sources as an enabling technology for learning based solutions have recently represented a significant shift from the cloud data centers to the ever-increasing edge devices, e.g., smartphones and industrial IoT devices. It is evident that these edge devices would push the AI solutions to the edge of the network to exploit the edge big data sources' potential entirely. In other words, just like cloud computing is distributed to the edge of 5G network, the artificial intelligence would also be distributed to the edge of 6G network. Therefore, an improved QoS and QoE would be guaranteed to the end users in terms of delay, user throughput and energy efficiency.

Following this direction here is proposed a new Hybrid AI Services Orchestrator (HAISO) model, which would ensure resilience and trustworthiness of open, large scale, dynamic services. To our best knowledge we did not find a similar model to be proposed. The HAISO would be primarily responsible for the composition of service elements available in the edge AI environment, such as, data analytics and data processing into more complex AI services, which could be offered to the end users. For some of the services may include sensing the traffic crowd sensing or planning the trip. The execution of such services is performed through multiple different components and entities that are spread in a wide area. This would increase the complexity in terms of decision-making process, particularly in the allocation of 6G network resources to achieve the QoS/QoE levels desired by the users. In order the execution of the AI services to be coordinated, it is necessary the orchestration mechanisms to be synchronized and combined from different service elements. Like that the QoS/QoE levels of a particular service, such as low latency, high user throughput and improved energy efficiency.

The HAISO would operate in a loosely coupled mode, which would consist with several levels: Edge AI Service Orchestrator (EAISO), Regional Domain AI Service Orchestrator (RDAISO), and Federated AI Service Orchestrator (FAISO), as it is shown in Figure 2.

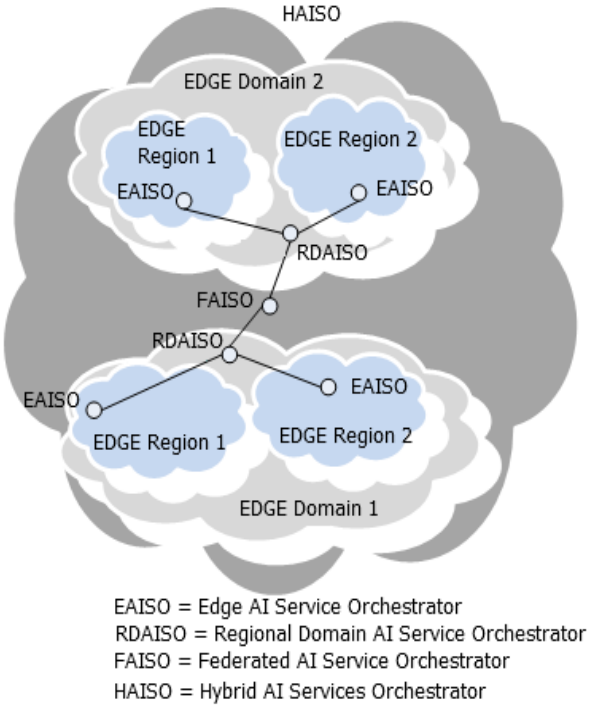


Fig. 2. Hybrid AI Services Orchestrator (HAISO) model for 6G network

The EAISOs are located at the edge of the network fog environment and enable semi-autonomous operation in different local edge regions. This allows the distribution of the load which provides scalability and much higher proximity to the end users with lower latencies.

The RDAISO is responsible for supervision of the EAISOs, within one edge domain. This level supports mechanisms that enable intra-domain cooperation between different local edge regions.

The FAISO is responsible for the management between different edge domains and allows a fruitful interaction among RDAISO modules. Such cooperation is enabled through various federation mechanisms implemented in FAISO module, which creates a multi-domain AI environment in 6G that should provide support of service ubiquity.

HAISO model provides flexibility and scalability, and it can be independently implemented in any network technology standard. It would possess its own federation machine learning mechanisms which would be implemented on all entities. In particular, the application of this model could be important for critical usage cases of IoT devices and Tactile Internet that requires 1 ms end-to-end latency to provide virtual-reality-type interfaces between humans and machines, and big data analytics that requires real time processing with stringent time requirement that can only be carried out in the fog.

5. 6G NETWORK ARCHITECTURE

An overview of the 6G network architecture that complies with the model described in the previous section together with the artificial intelligence is given on Figure 3.

AI data analytics is performed on the network which analyzes the collected historical data to get insights of the network status on the physical, medium access control (MAC), network and transport layer. It would provide network status and utilization opportunities. Work data which is obtained as an output of the network analytics processes would be used by Core data analytics for detecting and predicting the network anomalies to improve reliability and security of the network. The obtained data would be used to detect future faults based at historical and current information and network behavior.

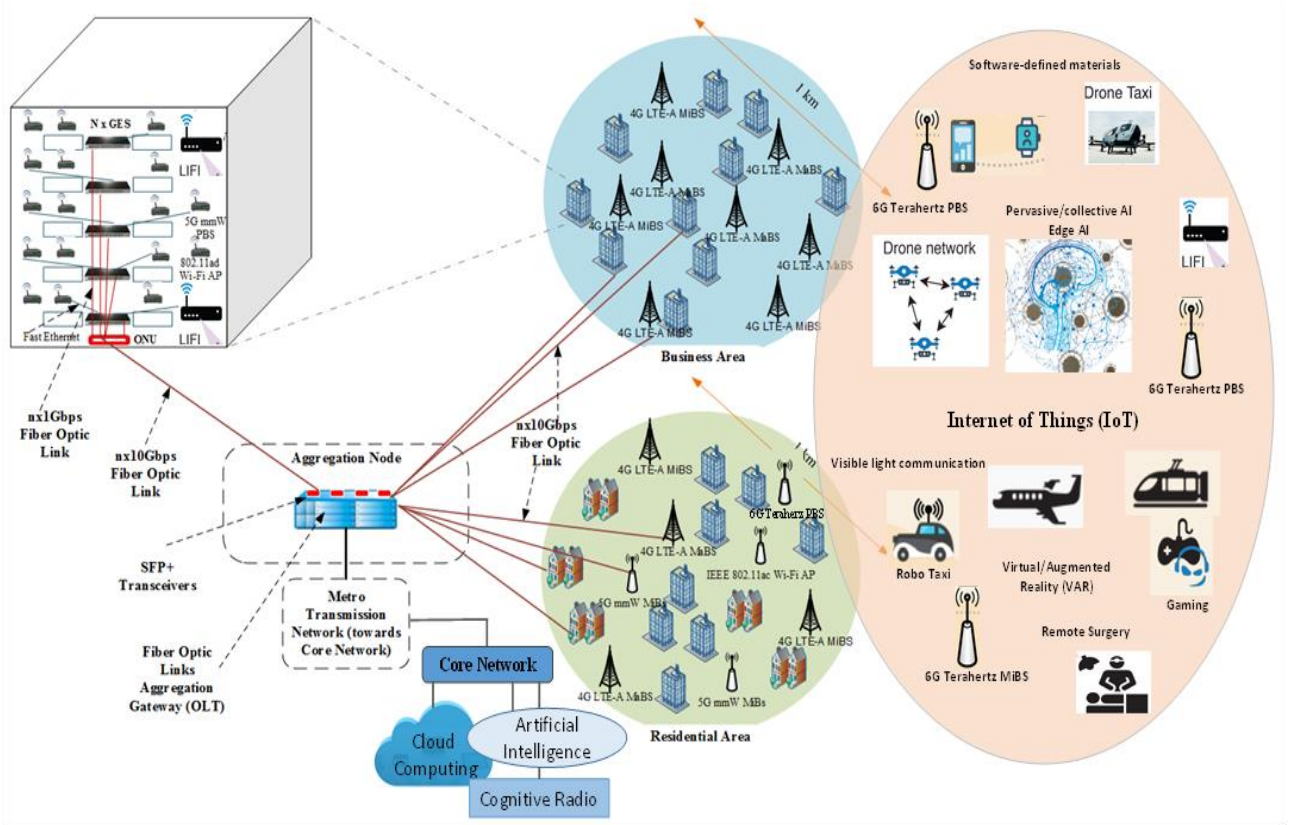


Fig. 3. 6G Advanced Wireless Mobile Heterogeneous Access Network (6G AWN-HAN) architecture with AI

Resource allocation solutions and notifications are expected to be output of this process. Predictive analytics would use data to forecast future resource availability based at user mobility prediction, traffic patterns and overload. It is expected optimized solutions to be proposed for allocation of the resources (open radio access network, i.e., ORAN and etc), network virtualization and slicing, edge computing, and optimization of virtual devices that consist of the network in order to offer ultimate network utilization, data transfer speed and traffic QoS. In some points core and predictive analytics may overlap. Even if this scenario looks naive it isn't, it must consider many parameters, i.e., big data deep learning mechanisms which need to be optimized if end-to-end traffic optimization is used.

In addition, there is an edge intelligence (EI) or edge AI located at the edge of the network. These edge devices would push the AI solutions to the edge of the network to exploit the edge big data sources' potential entirely.

6G networks would adopt ubiquitous AI solutions from the network core to the edge devices. However, the conventional centralized ML algorithms need the availability of a large amount of centralized data and training on a central server (e.g., cloud server or centralized machine). This would result with a bottleneck in the future ultra-large scale mobile networks [24]. Fortunately, federated learning (FL) which is an emerging distributed ML technique, is a promising solution to deal with this challenge and realize ubiquitous AI in the 6G networks. FL does not rely on storing all data to a central server where model training can occur. Instead, the innovative idea of FL is to train an ML model at each device (participant or data owner) where data is generated, or a data source has resided, and then let the participants send their individual models to a server (or aggregation server) and like that to achieve an agreement for a global model. However, despite the considerable potential advantages of FL for the 6G networks, FL is still in its infancy and encounter various challenges for fully operationalize in the 6G networks.

6. ENERGY EFFICIENCY IN 6G NETWORK

There are many ways to evaluate the quality of AI orchestrated services in 6G mobile networks. One of the most important QoS parameter is energy efficiency for the used bits per power consumption per user device, or vice versa.

The reduction of the power and power consumption by the networks and the devices is of vital importance for the economic and ecological sustainability in the industry. The general principle for minimizing of the power consumption at the network and the device should include all technology generations. This principle is recognized as an ecological goal and is quite important for the reduction of operating expenses in the network management [25]. In addition, the reduction of the power consumption would result to a longer battery life, which would contribute to a greater satisfaction of the mobile device users.

One of the possible methods to reduced power consumption in 6G mobile networks may be achieved by implementing the edge artificial intelligence.

The energy efficiency EE represents the amount of data that can be transfered through the power consumed per user, usually on a single cell, and represents the ratio between the user throughput R and the power P:

$$EE = \frac{R}{P}\left[\frac{\text{[bit/s/cell]}}{\text{[Joule/s/cell]}}\right] = \frac{R}{P}\left[\frac{\text{bit}}{\text{Joule}}\right]. \qquad (1)$$

In the relation (1) R is the user throughput which represents the quantity of data that can pass from source to destination in a specific time. The user throughput of a particular smart device R for network can be calculated as a ratio between the peak data rate $R_{\max}$ of the network and the number of the user devices N, proportional to some weight coefficient μ:

$$R = \mu \cdot \frac{R_{\max}}{N}. \qquad (2)$$

Here μ is a weight coefficient that models the bottleneck problem for the data that carry services from the AI computing data centers. The weight coefficient μ may receive any positive value between 0.7 and 1, and its value depends how much the AI data center is far away from the radio access network. If the AI data center is closer to the base station of the radio access network, then the coefficient μ has higher value close to 1, and if the cloud is at a greater distance from the base station of the radio access network, then the coefficient μ would have lower value. If the smart mobile device uses a service from edge AI networking intelligence, i.e., in the radio access network, then the weight coefficient μ is equal to 1.

In order to obtain the results of the user throughput the following values are used. The peak

data rate of 6G network in downlink is set to be equal at 1 Tbps in both downlink and uplink direction [19]. The number of the users is varied from 100 to 1000. The weight coefficient μ is randomly taken to be 0.85 in downlink direction and 0.75 in uplink direction.

The consumed power P on the other hand, can be expressed through the user throughput R with the following linear [26 – 27]:

$$P = \alpha R + \beta \tag{3}$$

Here α is the coefficient that gives the power necessary for data transfer (in downlink, or uplink direction), β is a coefficient that represents the idle power [28]. According 6G requirements given in [19] the energy efficiency is about to increase by a factor of 1000, and therefore the typical values for the coefficient α is taken to be 10^{-6} W/Mbit, and the value for the coefficient β is taken to be 10^{-5} W.

Simulation results are presented at Figure 4 and Figure 5. It can be noticed that 6G offers much higher energy efficiency by using the edge AI, rather than the AI in the core part. This means that much higher quantity of data can pass through 6G network by using edge AI, for lower power consumption.

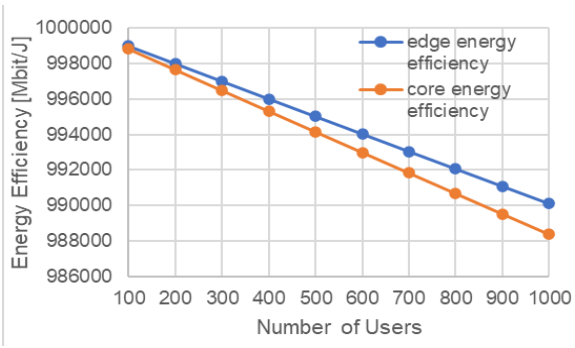


Fig. 4. A comparison of downlink energy efficiency in 6G network in both core and edge AI environment

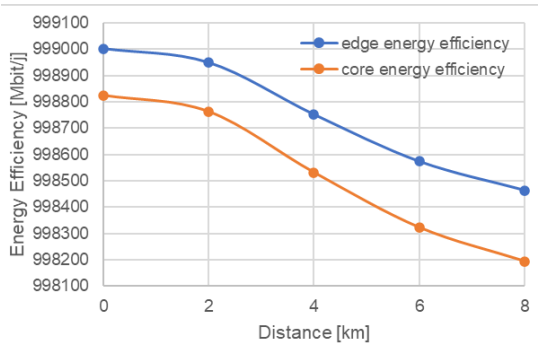


Fig. 5. A comparison of energy efficiency in 6G network in both core and edge AI environment, for 100 users

In addition, Figure 5 models the energy efficiency for 100 user devices, located at various distance from AI data center. Again, at every 2 km different modulation coding schemes, such as probabilistic constellation shaping, and QAM are applied. In other words, if the mobile device is closer to the AI data center than the energy efficiency is higher, because higher modulation coding scheme is applied, and therefore power consumption is lower and vice versa if the mobile device is getting more distant from the AI data center, then the energy efficiency is lowered because lower modulation coding scheme is being applied, and the power consumption is higher. Here again the energy efficiency is also higher if the service is being used by the edge AI, rather than the AI in the 6G core. Moreover in [29 – 31] it is stated that a basic goal of 6G communication is to operate battery-free whenever and wherever possible, with a target efficiency of 1 pico-joule per bit. And the simulation results given in Figures 4 and 5 nearly achieve this energy efficiency.

7. CONCLUSION

This paper proposed a 6G Advanced Wireless Mobile Heterogeneous Access Network (6G AWNHAN) architecture with artificial intelligence, whose description is expected to define the standard of 6G network. Furthermore, it evaluated the performance quality of artificially intelligently, orchestrated services in 6G mobile networks in terms of energy efficiency.

The obtained research results show a significant improvement in energy efficiency by applying artificial intelligence at the edge of the network. In particular, the big data analytics that requires real time processing and very often has stringent time requirement can only be carried out in the edge AI.

This is essential for critical usage cases of IoT devices and Tactile Internet where 1 ms end-to-end latency is required in the network to provide virtual-reality-type interfaces between humans and machines (human-machine interaction and machine-machine interaction). 6G network would provide an improved intelligent human-to-machine type of communication of real-time controlling IoT devices [21]. The tactile internet would enable humans and machines to exchange control, touch, and sense data in a real-time manner, which would provide support for haptics interface, as well as, possible visual feedback and remote response behavior that would be used in the industry, e-commerce, and many other possible applications.

Another critical application in 6G network is the holographic telepresence, which would enable users to enrich their traditional audiovisual communication with the sense of touch, while they are in different geographical locations. Holographic telepresence has very strict requirements such as terabits data rate (up to 4 Tb/s), ultra-low latency (less than 1 ms), and reliable communications, which cannot be supported by 5G networks.

In addition, new augmented and virtual reality applications such as haptic technology and virtual meeting room (VMR) which would transmit a large amount of real-time data, and would require very low end-to-end latency, which can be accomplished by implementing edge AI intelligence in 6G.

REFERENCES

[1] Mumtaz, S., *et al*. (2017): Terahertz communication for vehicular networks, *IEEE Transactions on Vehicular Technology*, vol. **66**, no. 7, pp. 5617–5625.

[2] ITU-R M.2370-0, IMT traffic estimates for the years 2020 to 2030, Jul. 2015.

[3] Nawaz, S. J., Sharma, S. K., Wyne, S., Patwary, M. N., Asaduzzaman, M. (2019): Quantum machine learning for 6G communication networks: state-of-the-art and vision for the future, *IEEE Access*, vol. **7**, pp. 46317–46350.

[4] Clemm, A., Vega, M. T., Ravuri, H. K., Wauters, T., De Turck, F. (2020): Toward truly immersive holographic-type communication: challenges and solutions, *IEEE Communications Magazine*, vol. **58**, no. 1, pp. 93–99.

[5] Du, J., Jiang, C., Wang, J., Ren, Y., Debbah, M. (2020): Machine learning for 6G wireless networks: Carrying forward enhanced bandwidth, massive access, and ultrareliable/low-latency service, *IEEE Vehicular Technology Magazine*, vol. **15**, no. 4, pp. 122–134.

[6] Strinati, E. C., Barbarossa, S., Gonzalez-Jimenez, J. L., Ktenas, D., Cassiau, N., Maret, L., Dehos, C. (2019): 6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication, *IEEE Vehicular Technology Magazine*, vol. **14**, no. 3, pp. 42–50.

[7] Jiang, D., Liu, G. (2017): An overview of 5G requirements, in *5G Mobile Communications*. Springer, pp. 3–26.

[8] Swarna Priga, R. M., Bhattacharya, S., Maddikunta, P. K. R., Somayaji, S. R. K., Lakshmanna, K., Kaluri, R., Hussien, A., Gadekallu, T. R. (2020): Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything, *Journal of Parallel and Distributed Computing*, vol. **14**, no. 2, pp. 16–26.

[9] Zhang, L., Liang, Y.-C., Niyato, D. (2019): 6G visions: Mobile ultrabroadband, super internet-of-things, and artificial intelligence, *China Communications*, vol. **16**, no. 8, pp. 1–14.

[10] Nayak, S., Patgiri, R. (2020): 6G: Envisioning the key issues and challenges, arXiv, preprint arXiv:2004.04024.

[11] Zhang, S., Liu, J., Guo, H., Qi, M., Kato, N. (2020): Envisioning device-to-device communications in 6G, *IEEE Network*, vol. **34**, no. 3, pp. 86–91.

[12] Tang, F., Kawamoto, Y., Kato, N., Liu, J. (2019): Future intelligent and secure vehicular network toward 6G: Machine-learning approaches, *Proceedings of the IEEE*, vol. **108**, no. 2, pp. 292–307.

[13] Gupta, R., Shukla, A., Tanwar, S. (2021): BATS: A blockchain and AI-empowered drone-assisted telesurgery system towards 6G, *IEEE Transactions on Network Science and Engineering*.

[14] Khan, L. U., Yaqoob, I., Imran, M., Han, Z., Hong, C. S. (2020): 6G wireless systems: A vision, architectural elements, and future directions, *IEEE Access*, vol. **8**, pp. 147 029–147 044.

[15] Lv, Z., Qiao, L., You, I. (2020): 6G-enabled network in box for internet of connected vehicles, *IEEE Transactions on Intelligent Transportation Systems*.

[16] Letaief, K. B., Chen, W., Shi, Y., Zhang, J., Zhang, Y. A. (2019): The roadmap to 6G: AI empowered wireless networks, *IEEE Communications Magazine*, vol. **57**, no. 8.

[17] Sliwa, B., Falkenberg, R., Wietfeld, C. (2020): Towards cooperative data rate prediction for future mobile and vehicular 6G networks, *Proc. 6G Wireless Summit (6G SUMMIT)*, Levi, Finland, pp. 1–5.

[18] Saad, W., Bennis, M., Chen, M. (2020): A Vision of 6G wireless systems: applications, trends, technologies, and open research problems, *IEEE Network*, vol. **34**, no. 8, pp. 134–142.

[19] Kitanov, S., Petrov, I., Janevski, T. (2021): 6G mobile networks: research trends, challenges and potential solutions, *Journal of Electrical Engineering and Information Technologies*, Vol. **6**, No. 2, pp. 67–77.

[20] Chen, M., Challita, U., Saad, W., Yin, C., Debbah, M. (2019): Artificial neural networks-based machine learning for wireless networks: A tutorial, *IEEE Communications Surveys & Tutorials*, vol. **21**, no. 4, pp. 3039–3071.

[21] Balali, F., Nouri, J., Nasiri, A., Zhao, T. (2020): Data analytics, In: *Data Intensive Industrial Asset Management*. Springer, pp. 105–113.

[22] Kibria, M. G., Nguyen, K., Villardi, G. P., Zhao, O., Ishizu, K., Kojima, F. (2018): Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks, *IEEE Access*, vol. **6**, pp. 32 328–32 338.

[23] Chen, M., Yang, Z., Saad, W., Yin, C., Poor, H. V., Cui, S. (2020): A joint learning and communications framework for federated learning over wireless networks, *IEEE Transactions on Wireless Communications*, to appear.

[24] Chen, M., Poor, H. V., Saad, W., Cui, S. (2020): Wireless communications for collaborative federated learning," arXiv, preprint arXiv:2006.02499.

[25] Heddeghem, W. V., Lambert, S., Lannoo, B., Colle, D., Pickavet, M., Demeester, P. (2014): Trends in worldwide ICT electricity consumption from 2007 to 2012, *Journal of Computer Communications*, vol. 50, pp. 64–76.

[26] Huang, J., Qian, F., Gerber, A, Morley Mao, Z., Sen. S., Spatscheck, O. (2012): A close examination of performance and power characteristics of 4G LTE networks. In: *Mobile Systems, Applications and Services (MobiSys 2012) Conference*, Low Wood Bay, Lake District, UK.

[27] Kitanov, S., Janevski, T. (2017): Energy efficiency of fog computing and networking services in 5G networks. In: *XVII IEEE International Conference on Smart Technologies EUROCON 2017*, Ohrid, Macedonia.

[28] Ragona, C., Granelli, F., Fiandrino, C. (2015): Energy-efficient computation of floading for wearable devices and

smartphones in mobile cloud computing. In: *IEEE Global Communications Conference (GLOBECOM)*.

[29] Mahdi, M. N., Ahmad, A. R., Qassim, Q. S., Natiq, H., Subhi, M. A., Mahmoud, M. (2021): From 5G to 6G technology: meets energy, internet-of-things and machine learning: A survey, *Applied Sciences*, vol. **11**, No. 8117.

[30] Huang, C., Hu, S., Alexandropoulos, G. C., Zappone, A., Yuen, C., Zhang, R., Renzo, M. D., Debbah, M. (2020): Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends, *IEEE Wireless Communications*, vol. **27**, no. 5, pp. 118–125.

[31] Liu, Q., Wu, J., Xia, P., Zhao, S., Chen, W., Yang, Y., Hanzo, L. (2016): Charging unplugged: Will distributed laser charging for mobile wireless power transfer work?, *IEEE Vehicular Technology Magazine*, vol. **11**, pp. 36 – 45.

Journal of Electrical Engineering and Information Technologies, Vol. **9,** No. 1, pp. 43–50 (2024)
Article 218
Received:May 2, 2024
Accepted: May 28, 2024
In print: ISSN 2545–4250
On line: ISSN 2545–4269
UDC: 621.39-028.27:34.04(497.7)
https://doi.org/10.51466/JEEIT2491218043d

Professional paper

REVIEW AND ANALYSIS OF NOVELTIES IN THE DRAFT TEXT OF THE NEW LAW ON ELECTRONIC COMMUNICATIONS

Liljana Denkovska[1], Valentina Angelkoska[2]

[1]*Agency of Electronic Communications, Skopje, N. Macedonia*
[2]*Faculty of Economics, "Ss Cyril and Methodius" University in Skopje, N. Macedonia*
angelkoskavalentina2@gmail.com

A b s t r a c t: The Law on Electronic Communications in N. Macedonia regulates the specific matter related to electronic communications. In the last few decades, there have been several versions of this law, the content of which is often changed and amended and is regularly harmonized with the regulation from the European Union. Currently, a draft text for a new Law on Electronic Communications is being prepared, with the aim of harmonizing it with the European Code of Electronic Communications (Directive 2018/1972, or COD Directive), adopted by the European Parliament and the Council of the European Union in December 2018. In this paper, after a brief introduction and overview of the Macedonian market of electronic communications, the reasons for adopting a new law are presented. The paper systematically presents and analyzes in detail the novelties that will be introduced with the new Law on Electronic Communications.

Key words: electronic communications; Law on electronic communications; networks; very high capacity networks; services, competition

ПРЕГЛЕД И АНАЛИЗА НА НОВИНИТЕ ВО НАЦРТОТ НА НОВИОТ ЗАКОН ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ

А п с т р а к т: Законот за електронски комуникации во С. Македонија ја регулира специфичната материја поврзана со електронските комуникации. Во последните неколку децении имаше неколку верзии на овој закон, чијашто содржина често е менувана и дополнувана и редовно усогласувана со регулативата на Европската Унија. Во тек е подготовка на предлог за нов закон за електронски комуникации, со цел негово усогласување со Европскиот законик за електронски комуникации (Директива 2018/1972, или COD-директива), кој Европскиот парламент и Советот на Европската Унија го донесоа во декември 2018 година. Во овој труд, по краткиот вовед и преглед на македонскиот пазар на електронски комуникации, презентирани се причините за донесување на нов закон. Трудот систематизирано ги презентира и детално ги анализира новините кои ќе се воведат со новиот закон за електронски комуникации.

Клучни зборови: електронски комуникации; закон за електронски комуникации; мрежи; мрежи со многу голем капацитет; услуги; конкуренција.

1. INTRODUCTION

Macedonian market of electronic communications creates total annual revenues of more than 300 million euros and it shows an increasing trend in the last few years. The market is mainly regulated by the Law on Electronic Communications [1], as well as other applicable laws.

The European Parliament and the Council of the European Union adopted the European Electronic Communications Code (Directive 2018/1972), or COD Directive on December 11, 2018 [2]. This Directive covers four directives: Directive 2002/19 [3], Directive 2002/20 [4], Directive 2002/21 [5], Directive 2002/22 [6] and Regulation (EC) No. 1211/2009 [7] of the European Parliament and of the Council of the European Union.

The convergence of the telecommunications, media and information technology sector means that all electronic communications networks and services should be covered by a single European Electronic Communications Code, established by a single Directive, while it is necessary to separate the regulation of electronic communications networks and services from the regulation of content. Therefore, this Directive does not cover the content of services provided over electronic communications networks, such as broadcasting content, financial services. and certain information society services.

In order to harmonize the existing regulation for electronic communications in the Republic of N. Macedonia with this directive, the Minister of Information Society and Administration of the Republic of N. Macedonia has established a working group for the drafting of a new Law on Electronic Communications in 2023. The draft text of this law was prepared and published on ENER system [8] in order to receive opinions and comments from all interested parties.

The draft text of the Law on Electronic Communications is structured in 19 chapters, and this paper lists and analyzes the novelties in relation to the existing Law on Electronic Communications that are proposed and implemented in this draft text of the new law. The paper is organized as follows: in Section 2 we summarize the trends of the Macedonian market of electronic communications and the main reasons for the adoption of the new Law on Electronic Communications; in Section 3 novelties in the new law are analyzed in details. Finally, we present our concluding remarks in Section 4.

2. TRENDS IN MACEDONIAN MARKET OF ELECTRONIC COMMUNICATIONS AND SUMMARY OF REASONS FOR ADOPTING THE NEW LAW

As mentioned in the introduction, Macedonian market of electronic communications creates total annual revenues of more than 300 million euros in the recent years, showing an increasing trend. Total annual revenues of the Macedonian market of electronic communications for the period 2010–2022 is presented in Figure 1, according to the annual reports on the development of the Macedonian market of electronic communications [9] published by the Agency for Electronic Communications (www.aec. mk). After the obvious decreasing trend in the period 2010–2015, followed by a relatively stable period (2015–2021), the market has increased by 6.8% in 2022.

Figure 2 presents the number of notified and active entities participating in the Macedonian market of electronic communications in 2022, distributed in the defined seven services (S1–S7).

The annual report for 2023 is expected to be published by the Agency for Electronic Communications in October 2024.

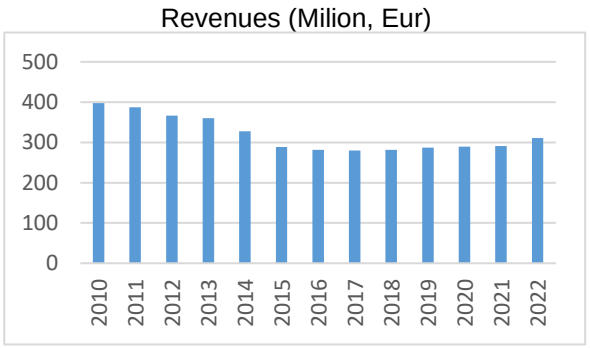


Fig. 1. Total annual revenues in the Macedonian market of electronic communications in the period 2010–2022 (*Source*: Agency for Electronic Communications – www.aec.mk)

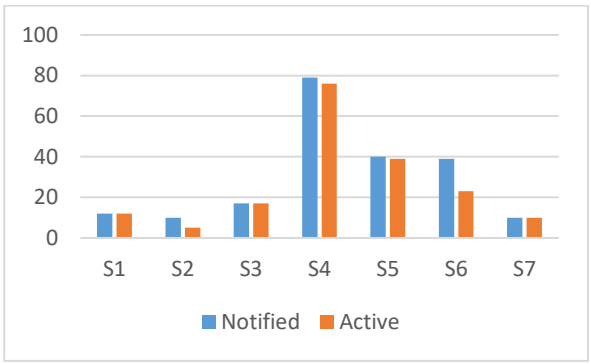


Fig. 2. Number of notified and active entities participating in the Macedonian market of electronic communications in 2022 (*Source*: Agency for Electronic Communications – www.aec.mk)

In a small economy, as it is the Macedonian case, a market of such size is a significant contributor, so the analyses of the applicable laws which regulate the market and consequently can significantly affect the market, are highly relevant. This market is mainly regulated by the Law on Electronic Communications, which is in a constant process of harmonization with the directives of the European Union.

In addition to compliance with the COD Directive, mentioned above, the main reasons for

adopting the new Law on Electronic Communications, are listed below:

- Encouraging the development of electronic communication networks and services in order to ensure economic and social development;
- Encouraging investments in public electronic communication networks by introducing new technologies and services, especially networks with very high capacity;
- The protection of the rights of end users, including end users with disabilities and end users with special social needs;
- Ensuring efficient and sustainable competition;
- Interoperability of electronic communication services;
- Provision of universal service;
- Effective use of the radio frequency spectrum and numbering; and
- Ensuring the security of networks and services.

3. ANALYSIS OF THE NOVELTIES IN THE NEW LAW ON ELECTRONIC COMMUNICATIONS

In the following subsections, the proposed novelties in the new Law on Electronic Communications are analyzed in details, according to the structure of the draft text, organized in 19 chapters.

a) Chapter I – *General provisions*

In Article 3 of this Chapter of the law, which refers to definitions, terms and expressions used therein, the existing definition of publicly available telephone service is replaced by the definition of voice communication service. This is because technological and market developments have led more and more networks to switch to Internet protocol (IP) technology, allowing end users to choose from a number of competing voice service providers. Therefore, the term "publicly available telephone service" is considered to refer to traditional analog telephone services and should be replaced by the modern and technologically neutral term "voice communication service". The nature of this service is its bi-directionality, which allows both parties to communicate, and also includes communication tools specifically intended for end users with special needs who use text or full chat services.

In this direction, new definitions are introduced such as: Communication service between persons, Communication service between persons that uses numbering, and Communication service between persons that does not use numbering.

The definition of Subscriber is replaced by the definition of Consumer, and due to its compliance with the Law on Consumers of the Republic of N. Macedonia.

In addition to the term operator, a new term network operator is introduced, which covers not only the legal entities that provide public electronic communication networks, but also the legal entities that provide physical infrastructure, such as production, transport or distribution services of gas, electricity, including public lighting, heating, water, discharge or treatment of waste water and sewage, and drainage systems, as well as transport services such as: railways, roads, ports, and airports.

In order to ensure more efficient communication with emergency call services, new definitions are introduced such as: public safety answering point (PSAP) and most appropriate PSAP.

New definitions are also being introduced that clarify the concepts of digital radio and digital television.

b) Chapter II – *Jurisdiction over electronic communications*

Number in order to ensure a distinction between policies and regulatory activities in the field of electronic communications, as a competent authority, in addition to the ministry responsible for matters in the field of electronic communications and the Agency for Electronic Communications, the Government of the Republic of N. Macedonia is also involved with decisively and taxatively determined competences.

This part of the draft text of this law determines the general goals that the Agency for Electronic Communications should achieve in order to ensure their achievement. The goals are presented in Table I.

The provisions relating to the Agency for Electronic Communications, as an independent, non-profit regulatory body of the markets for electronic communications in the Republic of N. Macedonia, its competence, the accountability for its work which it presents to the Parliament of the Republic of N. Macedonia by submitting a report, no later than 31 March in the current year, the transparency and influence of the public in relation to its operation, remain unchanged.

T a b l e 1

General goals of the Law on Electronic Communications

No.	Goal
1.	Access and use of networks with very high capacity.
2.	Promotion of competition in the provision of electronic communication networks and associated facilities, including effective competition in the infrastructure and in the provision of electronic communication services and related services.
3.	Removing obstacles and creating conditions for investment in electronic communication networks, electronic communication services, associated facilities, and services throughout the country.
4.	Provision of predictable regulation.
5.	Promotion of efficient, effective and coordinated use of the radio frequency spectrum.
6.	Open innovation approach.
7.	Creation and development of trans-European networks.
8.	Ensuring availability and interoperability of pan-European services and "end-to-end connectivity".
9.	Ensuring connectivity, widespread availability and use of very high capacity networks, including fixed, mobile and wireless networks and electronic communication services.
10.	Creating maximum benefits in terms of choice, price and quality based on effective competition.
11.	Maintaining the security of networks and services.
12.	Providing a high level of protection to end users taking into account their needs, such as affordable prices, especially for disabled end-users, elderly end-users, and end-users with special social needs, as well as the possibility of choice and equivalent access for disabled end-users.

The Commission for Electronic Communications and the Director of the Agency for Electronic Communications are again determined as organs of the Agency in this text of the draft law, so that in the conditions for appointing members of the Commission, the previous prerequisite for at least five years of appropriate work experience in the profession are replaced by at least 10 years.

The National Center for Response to Computer Incidents (MKD-CIRT), established in Article 28 of the draft text of this law, which was established by the existing Law on Electronic Communications [8], as a separate organizational unit within the Agency for Electronic Communications, continues to perform its function until the expiration of the term of two years from the date of entry into force of the Law on Security of Network and Information Systems and Digital Transformation in the Republic of N. Macedonia [10].

c) Chapter III – *Fees*

The provisions of this chapter of the draft law, which refer to the financing of the Agency for Electronic Communications remain unchanged, with the exception of the provisions that refer to the financing of the Operational Technical Agency (OTA), which are deleted in this draft text of the law.

d) Chapters: IV – *Supervision*, V – *Penalty authority*, VI – *Dispute resolution, and* VII – *Delivery, recording, storage, and publication of data and information*

The provisions relating to the competence of the Agency for Electronic Communications to supervise operators and other legal and natural persons who perform activities of providing electronic communication networks and/or services from Chapter IV of this law, remain unchanged.

In the same fashion, there are no changes in the provisions of Chapter V, by which the Agency for Electronic Communications is determined as the competent penalty authority, and the provisions of Chapter VI, which regulate the procedure for resolving disputes led by the Agency for Electronic Communications between operators, network operators and operators, and between end-users and operators. Provisions of Chapter VII regarding delivery, recording, storage, and publication of data and information, also remain unchanged.

e) Chapter VIII – *Conditions for provision of electronic communication networks and/or services*

The provision of electronic communication networks and/or services in the territory of the Republic of N. Macedonia, in accordance with the provisions of this chapter of the law, is free, after prior registration of the legal or natural person who intends to provide public electronic communication networks and/or services and on the basis of a notification submitted to the Agency for Electronic Communications, before starting, that is, after a change or termination of the provision of public electronic communication networks and/or services. The provision of public electronic communication networks and/or services can be limited, if necessary, due to the application of special regulations

that provide for special treatment for foreign nationals, which is justified for the protection of public order, public safety, or human health.

f) Chapter IX – *Construction of electronic communication networks and associated facilities*

Public electronic communication networks and associated facilities, interfaces and other network elements should be planned, designed, built, maintained and operated in accordance with this law, regulations adopted on the basis of it, spatial planning and building regulations, regulations for the protection of the environment, as well as the regulations, standards and/or technical specifications contained in the recommendations of the European Union.

In order to ensure broadband access to the Internet, the draft text of this law introduces new provisions, established in Article 64 thereof, which refer to the obligations of the Electronic Communications Agency to manage, regularly implement and update it, at least every three years, the geographic review of the availability of electronic communication networks that can provide broadband access to the Internet. The geographic review includes a review of the geographic availability of the existing broadband networks in the territory of the Republic of N. Macedonia, and also includes the planned coverage with broadband networks, which cannot be longer than three years, including the networks with very high capacity, as well as data for significant upgrades or network expansion, to achieve data transfer of at least 100 Mbit/s.

In order to encourage investment and installation of elements of electronic communication networks to ensure transmission at high speeds, with the provisions of Article 69 of this law, an obligation is imposed on each network operator, based on a received written request from an operator of public electronic communication networks to provide access to its physical infrastructure, under fair and reasonable conditions and prices.

The provisions of Article 70 of this law, which refer to the Single Point of Information (SPI – ETI) that the Agency provides through a publicly available GIS platform, are unchanged.

g) Chapter X – *Ensuring competition*

The provisions of this chapter of the law aim to reduce the number of ex-ante regulatory obligations and ensure that electronic communications are regulated solely by the Law on Competition [11]. Given that electronic communications markets have been characterized by highly dynamic competition in recent years, it is necessary to impose ex-ante regulatory obligations only if there is no effective and sustainable competition. In order to provide adequate incentives for investing in new networks with very high capacity, to support innovations in Internet services rich in content, in addition to the obligations established in Articles 78 and 79 of this law, the Agency for Electronic Communications, may impose to operators who have control of access to end users, an obligation for interconnection, if it has not been established, an obligation for interoperability of services, an obligation to provide access to application program interfaces and/or to an electronic program guide, and also upon receiving a reasonable request, to impose an obligation to provide access to wire and cable installations, as well as to the associated facilities in buildings, or to the first point of concentration or distribution. The Agency for Electronic Communications may also impose on the operators an obligation for joint use of the passive infrastructure, or an obligation to conclude a contract for providing local roaming access.

h) Chapter XI – *Regulation of operators with significant market power*

In order to ensure competition in the markets for electronic communications in the Republic of N. Macedonia and to reduce or completely remove barriers to the entry of new operators, the Agency for Electronic Communications, based on an analysis of the relevant markets, determines operators with significant market power which may be imposed an obligation for transparency during interconnection or access, an obligation for non-discrimination during interconnection or access, an obligation to keep separate accounting during interconnection or access, an obligation to access and use built infrastructure, an obligation to ensure access and use of specific network assets, price control, and cost accounting obligation. In the draft text of this law, with the Article 94, a new obligation is introduced for the regulation of new network elements with a very high capacity. With this obligation, it is possible for operators who have been determined as operators with significant market power in one or more relevant markets to submit an offer to the Agency for Electronic Communications to undertake obligations that will enable joint investment in setting up new networks with very high capacity, consisting of fiber optic elements to the end user area or base station. The joint investment obligation includes an offer for co-ownership or long-term risk sharing,

through joint investment or through entering into a purchase and/or sale agreement with other operators.

The provisions relating to the obligation for functional separation, voluntary separation from a vertically integrated operator, have not changed.

Article 97 of the draft text of this law proposes a procedure for accepting obligations, according to which an operator with significant market power can submit to the Agency for Electronic Communications an offer for accepting obligations, applicable to its network, and related to the access conditions and/or the terms of the joint investment.

New provisions are introduced in Article 98 of this law, which regulate only wholesale operators. With them, it is determined that the Agency for Electronic Communications can designate an operator that is not present in any retail market, as an operator with significant market power in one or more wholesale markets.

The provisions relating to the regulation of the existing infrastructure and the regulation of retail services have not been changed.

i) Chapter XII – *Provision of universal service*

With the provisions of this chapter of the Law on Electronic Communications it is possible for the consumers of electronic communication services in the Republic of N. Macedonia to have access at an affordable price to an available and adequate service for broadband access to the Internet and a service for voice communication, with an appropriate quality of service, including basic connection at a fixed location, and the Agency for Electronic Communications can impose an obligation for affordable prices for services that are not provided at a fixed location, for the sake of full social and economic inclusion of consumers.

The prices of individual universal services should be affordable and the same throughout the territory where the designated operator provides the universal service.

Unlike the existing legal solution, with Article 105 of the draft text of this law, as other universal services for which, if the Agency for Electronic Communications deems it necessary, the following are determined: a complete directory for all end users, access to the service for providing information for the numbers of end users and public payphones.

Provisions relating to cost control, compensation of the net costs of providing universal service and the universal service compensation fund, remain unchanged.

j) Chapter XIII – *Rights of end-users*

One of the most essential issues that are regulated by the existing Law on Electronic Communications, and regulated in more details in the draft text of the new Law on Electronic Communications, are the issues of the rights of end users when using electronic communication services. The contracts that operators conclude with end users are an important tool for ensuring transparency and legal certainty for end users. Therefore, in the draft text of the law, special emphasis is placed on the obligation of operators of publicly available communication services, with the exception of transmission services used to provide machine-to-machine services, in a clear and comprehensible manner, available on a durable medium or in a document that is easily accessible and simple for electronic download, before concluding a contract, provide the end-user with all of the informations, in particular about: the main characteristics of each offered service, the minimum quality level of the offered service, price information, information for the duration of the contract, the conditions for its extension and termination, as well as for the possible compensations in case of termination of the contract.

In this direction, of particular importance is the provision that imposes on the operator who provides an internet access service or a publicly available communication service between persons, and is charged based on the duration or amount of consumption, the obligation to enable the end users monitoring and controlling the use of each of the contracted services, that is, to notify the end user before he reaches the limit in terms of duration or amount of consumption.

In the same direction of securing the rights of end users, there are also the provisions with which the Agency for Electronic Communications is obliged, through its website, to provide end users with access to an independent comparison tool that will enable them to compare and evaluate the different services, in terms of prices and quality of services.

In terms of ensuring the quality of services, a novelty in this draft text of the law is the provision that obliges the operator for its electronic communication network with a very high capacity, based on optics, to have a technical report from measurements of the quality parameters, which are issued by an appropriate accredited inspection body at a higher educational institution in the field of electronic communications.

k) Chapter XIV – *Radio frequency spectrum*

The radio frequency spectrum is a limited natural resource, a public good with significant social, cultural and economic value. The radio frequency spectrum of the Republic of N. Macedonia is managed by the Agency for Electronic Communications.

The provisions for the Radio Frequency Spectrum Allocation Plan, the Plan for Allocation and Use of Radio Frequencies, the principle of neutrality in relation to technologies, the principle of neutrality in relation to services, the conditions for the use of radio frequencies, as well as the procedures for issuing approval for the use of radio frequencies are also implemented in this draft text of the law.

This part of the law contains the provisions that refer to the renewal of the approval for the use of radio frequencies. With them, it is proposed that the Agency for Electronic Communications, ex officio or at the request of the holder of the authorization for the use of radio frequencies, determine whether there is a need for its renewal. If the holder of the authorization for the use of radio frequencies submits a request for the renewal of the same, it can do so at least five years, and at the latest one year before the expiration date of the validity of the authorization, and the Agency can ex officio carry out an evaluation procedure of the need to renew the authorization for the use of radio frequencies, at least two years before the expiration of the validity period of that authorization. If the Electronic Communications Agency makes a decision to renew the approval, it will issue a new approval to the holder of the approval for the use of radio frequencies, in which it can modify some of the conditions for the use of radio frequencies and oblige the holder to pay a one-time fee for the use of radio frequencies.

New provisions in the draft text of the Law on Electronic Communications are also the provisions for the duration and extension of the authorization for the use of radio frequencies. They regulate that the duration of the authorization for the use of radio frequencies for the provision of wireless broadband communication services cannot be shorter than 15 years, nor longer than 20 years. The Agency for Electronic Communications, at least two years before the expiration of the validity period of the approval, will carry out a procedure in order to evaluate whether there are conditions for extending the validity of the approval for the use of radio frequencies, while it may also decide to amend the terms of use of radio frequencies.

Another novelty in this part of the law are the provisions that refer to access to the radio local network (RLAN). These provisions prohibit operators of public electronic communications networks and/or services from restricting or preventing an end user from accessing an RLAN of their choice, or from providing other end users with access to their RLAN networks. Also new in this chapter of the law are the provisions for the installation and operation of short-range wireless access points. These provisions propose that operators have access to any physical infrastructure owned or operated by a public sector institution that is technically suitable for the deployment of a short-range wireless access point.

l) Chapters: XV – *Numbering*, XVI – *Digital radio and television services*, XVII – *Radio equipment and telecommunications terminal equipment*

The provisions implemented in these chapters of the law are taken from the existing Law on Electronic Communications.

m) Chapter XVIII – *Security and integrity of public electronic communication networks and services and protection of personal data*

The provisions of this chapter of the law, and especially the provisions of Article 186, will be applied until the day of entry into force of the Law on Security of Network and Information Systems and Digital Transformation of the Public Sector in the Republic of N. Macedonia [10].

n) Chapter XIX – *Penalty provisions*

This chapter of the Law on Electronic Communicationsis harmonized with the Law on Misdemeanors [12].

4. CONCLUDING REMARKS

The paper presented and analyzed in details the novelties that will be introduced with the new Law on Electronic Communications in N. Macedonia. Currently, a draft text for a new Law on Electronic Communications is being prepared, with the aim of harmonizing it with the European Code of Electronic Communications (Directive 2018/1972, or COD Directive), adopted by the European Parliament and the Council of the European Union in December 2018. The process of preparation started in 2023, initiated by the Minister of Information Soci-

ety and Administration of the Republic of N. Macedonia, who has established a working group for this task. The first draft text of the new law was published on ENER system in January 2024 and it has received number of opinions and comments from all interested parties. The process of preparation/adoption of the new proposed law is postponed due to current election processes in the country. The content of the proposed new law on Electronic Communications might be further modified, depending on the comments from the interested parties, strategy of the new government, as well as the status and the final content of the proposed new law on the Law on Security of Network and Information Systems and Digital Transformation. When adopted, it is expected that the goals of the new Law on Electronic Communications, elaborated in this paper, will be achieved during its implementation.

REFERENCES

[1] *Law on Electronic Communications*, Official Gazette of the Republic of Macedonia No. 39/14, 188/14, 44/15, 193/15, 11/18, 21/18, Official Gazette of the Republic of N. Macedonia No. 98/19, 153/19, 92/21.

[2] *Directive (EU) 2018/1972* of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), Text with EEA relevance. https://eur-lex.europa.eu/eli/dir/2018/1972/oj

[3] *Directive 2002/19/EC* of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0019

[4] *Directive 2002/20/EC* of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0020

[5] *Directive 2002/21/EC* of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0021

[6] *Directive 2002/22/EC* of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0022

[7] *Regulation (EC) No 1211/2009* of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32009R1211

[8] Draft text of the new *Law on Electronic Communications*, https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=83184

[9] *Annual Reports on the Development of the Macedonian Market of Electronic Communications*, Agency for Electronic Communications. https://aek.mk/en/category/izveshtai/godipni-izveshtai-za-analiza-na-pazar/

[10] Draft text of the *Law on Security of Network and Information Systems and Digital Transformation*. https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=80751

[11] *Competition Law*, Official Gazette of the Republic of Macedonia No. 145/2010, 136/11, 41/14, 53/16, 83/18).

[12] *Law on Misdemeanors*, Official Gazette of the Republic of Macedonia No. 96/2019.

Journal of Electrical Engineering and Information Technologies, Vol. **9,** No. 1, pp. 51–61 (2024)
Article 219
In print: ISSN 2545–4250
Received: May 7, 2024
On line: ISSN 2545–4269
Accepted: May 30, 2024
UDC: 004.491.056:34.05(4-672ЕУ:497.7)
https://doi.org/10.51466/JEEIT2491219051a

Professional paper

CYBER SECURITY LEGAL FRAMEWORK WITH SPECIAL FOCUS ON NIS2 AND N. MACEDONIA

Valentina Angelkoska[1], Ivo Paunovski[2]

[1] *"Ss. Cyril and Methodius" University in Skopje, Faculty of Economics, Skopje, N. Macedonia*
[2] *A1 Macedonia, Skopje, N. Macedonia*
angelkoskavalentina2@gmail.com

A b s t r a c t: The digitization trend and the complex geopolitical situation result in an increased number of cyber attacks worldwide. The countries of the Western Balkans, including N. Macedonia, are no exception to this trend. The subjects of the cyber attacks are the critical infrastructure and data privacy of public and private companies. One of the major issues that N. Macedonia is facing in the domain of cyber security is the lack of an effective legislative framework that will be harmonized with the legislative frameworks of the EU member states. This paper provides an overview of European legislation with a special focus on NIS2 Directive and the actions that regulated companies should undertake in order to meet the requirements of this directive. Apart from an overview of the Macedonian cyber security related legislation, this paper also provides appropriate recommendations for governments and key stakeholders about cyberspace and critical infrastructure protection.

Key words: critical infrastructure; cyber attacks; NIS2 Directive; strategy

ПРАВНА РАМКА ЗА КИБЕР БЕЗБЕДНОСТ СО ПОСЕБЕН ФОКУС НА ДИРЕКТИВАТА NIS2 И С. МАКЕДОНИЈА

А п с т р а к т: Трендот на дигитализација во рамките на општеството и сложената геополитичка ситуација резултираа со пораст на бројот на кибер напади во светски рамки. Земјите од Западен Балкан, вклучително и С. Македонија, не се исклучок од ова правило. Предмет на овие кибер напади се критичната инфраструктура и приватноста на податоците на јавните и приватните компании. Едно од главните прашања со кои се соочува С. Македонија во доменот на кибер-безбедноста е немањето на ефективна законодавна рамка усогласена со законските рамки на земјите членки на ЕУ. Во овој труд е даден приказ на европската легислатива со специјален фокус на Директивата NIS2 и на активностите што регулираните компании треба да ги преземат за да ги исполнат барањата од оваа директива. Освен преглед на македонската легислатива во доменот на кибер-безбедноста, овој труд дава и соодветни препораки со цел подигнување на нивото на безбедноста на критичната инфраструктура.

Клучни зборови: кибер-напади; критична инфраструктура; Ддиректива NIS2; стратегија

1. INTRODUCTION

The number of connected devices on the Internet in EU in 2022 is estimated to be almost 2.7 billion [1]. About 440 (four hundred and forty) million inhabitants live within the European Union, and 90% of them own a smartphone, a personal computer and an Internet connection. On top of it, nearly 95% of companies and public authorities are also connected to the Internet.

The digital revolution and its use by governments, people, private and public enterprises, criminal groups and non-state actors, have increases the exposure to cyber risks. It is estimated that every 40 seconds, companies, and public bodies are victim of a cyber-attack. The World Economic Forum claims

that cyber attacks and cyber warfare are the most serious threats concerning cyberspace. According to [2], the most prevalent violations in cyberspace have been fake news during the Covid-19 pandemic, information security breaches, propaganda, threats, and hate speech. Recently, a large number of cyber-attacks on state institutions and critical infrastructure have been published in the media. Therefore, cyber attacks are no longer seen only as an IT problem but also as a social problem [3]. For example, recently the Irish healthcare system was the target of a ransomware attack that disrupted the operation of the healthcare system. The victim of a cyber attack was also the largest gas distributor in US, due to which the gas distribution in 8 (eight) American states was disrupted for a certain period of time.

Cyber adversaries' level of sophistication, persistence, and technical capability to attack the systems that support critical infrastructure is on the rise in Western Balkans countries as well. In the last few years, companies and state institutions in Macedonia are also frequent targets of cyber attacks. We have been witnesses of a successful cyber attacks on many private companies, banks and also large state institutions like Health Insurance Fund, the Agency for Electronic Communications, the Agency for Real Estate Cadaster and MEPSO. Most of these attacks originate outside the territory of the Western Balkans. The consequences of successful cyber attacks, apart from the damage to the company itself, directly and/or indirectly affected other companies and natural persons. Therefore, it is critical for private companies and Macedonian government to be aware of such violations in order to better understand the need for investment in cyber security expertise.

Taking any protective measures is associated with the generation of costs. Bearing in mind that generation of profit is built in the core of the existence of any private company, making any business decisions are made based on the analysis of costs and potential profit [4]. On the cost side, only the costs related to the remediation of damage caused by the cyber attack and estimation of the damage to the reputation of the brand are usually calculated. Companies typically do not take into account the impact of a cyber attack on other businesses or society itself. Failure or unwillingness to calculate these costs contributes to inadequate investment in network and information system security. Compensation for damage caused by the violation of legal rights of other businesses that are closely related to the affected company are ineffective [5]. Therefore, European Union introduced a series of regulations that require companies to introduce certain standards and norms related to cyber protection [6].

2. EU CYBER SECURITY LEGAL FRAMEWORK

The origins of cyber security legislation date back to 2008, when the first draft version of European Critical Infrastructure Directive (ECI) was prepared, aimed at transport and energy infrastructure. This directive represents a basis for future texts in terms of defining a common approach, although the risks related to cybersecurity were not part of this directive.

The cornerstone of the common cyber security policy was born in 2013 with the adoption of the first EU Cyber Security Strategy (EUCSS) [7]. The EUCSS is the first official document published by the EU where the term "cyber security" is used for the first time. According to this strategy, the EU has instructed each member state to implement a National Computer Emergency Response Team (CERT) as a competent cyber security authority that will represent the country in discussions at European level.

In 2016, the Network and Information Systems directive (NIS) was adopted [8]. This directive applied to Digital Service Providers (DSP) and Operators of Essential Services (OES). The scope of the NIS directive was applicable to 7 (seven) different sectors. The aim of this directive was to ensure a high and common level of security of EU networks and information systems. The cyber-resilient program was developed based on three main pillars:

- Improving national cyber security capabilities;
- Building cooperation at EU level;
- Promoting a culture of risk management and incident reporting.

In accordance with the NIS directive, each of the member states created a NIS Cooperation Group. The work of these NIS groups is coordinated by European Union Agency for Cybersecurity – ENISA (www.enisa.europa.eu). The main duty of ENISA is achieving a high common level of cyber security across Europe. Also, ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services, and processes with the introduction of cyber security certification schemes. The NIS directive showed its limitations during the "Covid-19" crisis, given that this period was represented by rapid digital transformation of the society. Therefore, the EU Commission decided to work on the NIS2 directive which was adopted in 2023 [9].

Maybe the most significant step in regards of European legislation is the adoption of the GDPR (General Data Protection Regulation), a regulation that refers to the protection of personal data [10]. The GDPR regulation adopted in 2016 is the first European regulation that focuses on the unification of legislation among all EU member states when it comes to the protection of users' personal data and establishes sanctions in case of non-compliance with such obligations. In accordance with the GDPR regulation, the Digital Services Act (DSA) [11] was adopted in 2022. With this law, all digital companies and online intermediaries offering their services in the EU Single Market, regardless of whether they are established in the EU or outside it, must comply with obligations related to transparency and cooperation with national authorities. In case of non-compliance, fines and sanctions can amount to up to 6% of the platform's annual turnover. Since the Digital Services Act (DSA) had certain shortcomings, in 2022 the Data Governance Act (DGA) [12] was adopted. The objective of this act was to create a single European data market and the promotion of confidential data sharing. This act is generally focused on specific sectors such as health, energy, transport, supply chain. It is important to note that with this act the use of artificial intelligence (AI) begins to be regulated for the first time. The main purpose of enacting the DGA is to give some power to small and medium-sized enterprises compared to the power that digital leaders have given that it addresses the need to seek and give consent by the individuals in case their personal data needs to be processed. This act also applies to other data holders who should now allow the use of non-personal data for the purposes of general interest, i.e., scientific research or improving the public services without any compensation. What is particularly important to note here is that whenever it comes to data transfer it is necessary to ensure compliance with the GDPR regulation.

In order to speed up the digitization process in EU, in 2014 the eIDAS regulation [13] was passed which enabled EU citizens to use a national electronic identification (eID) scheme, such as ItsMe in Belgium, to access public services online not only in Belgium but also in other countries within the European Economic Area. In 2021, the European Commission introduced eIDAS 2.0 which enabled the addition of digital wallets to eIDAS. Digital wallets are applications and services that enable secure digital identity management.

Within the framework of the banking and financial sector, the EU adopted two directives:

- Payment Services Directive 2 (PSD2) [14] has established guidelines on major incident reporting, setting out the criteria, thresholds, and methodology to be used by payment service providers (PSP) to determine whether an operational or security incident should be considered major or not and accordingly defined the procedure for notification of the Member State's competent authority.
- Digital Operational Resilience Act (DORA**)** [15], which defines uniform requirements for the security of the networks and information systems of companies and organizations active in the financial sector as well as critical the third parties that provide services related to ICTs.

After the adoption of EUCSS in 2013, the second cornerstone of the EU cyber security legislation was related to the introduction of EU Cybersecurity Act (EU CS Act) [16] in 2019, bringing forward awareness on the new needs in terms of cyber security, resilience, and cooperation in the EU. EU CS act is having two focus points:

- The European Certification Framework providing companies set of rules, technical requirements, standards, and procedures;
- Strengthening the European Network Information Security Agency (ENISA), European Union Agency for Cyber security.

In December 2020, the EU published its second Cyber Security Strategy (EUCSS). This new strategy was adopted in order to provide guarantees for a global and open Internet by implementing strong safeguards in case of cyber security risks. This strategy today is probably best known for the announcement of NIS2 Directive.

From artificial intelligence regulation point of view, the Law on Artificial Intelligence (AI Act) was adopted, which ensures the introduction of a common legal framework that applies to all types of systems and to all sectors except the military sector. The AI Act banned unacceptable practices, such as manipulating people through subliminal techniques or remote real-time biometric identification. The latest regulation passed by the EU is the Cyber Resilient Act (CRA). The CRA aims to improve transparency in the security domain of hardware and software products by introducing a coherent cyber security framework within which hardware and software manufacturers remain accountable for cyber security throughout the entire lifecycle of their products. The CRA aims to complement the AI Act, the CSA and the NIS2 Directive.

In recent years, intensive activity can be observed within the framework of EU legislation aimed at raising the level of cyber security in EU member states. Table 1 shows the time line of EU cyber security legal framework while the Figure 1 represent a simplified view of the overall legislation produced by the EU. In the next part of this paper we will look a little more at what improvements NIS2 offers in relation to the NIS Directive and what companies need to do to be ready when this directive comes into force.

T a b l e 1

Timeframe of EU cyber security legal framework

Year	Act
2013	EUCSS
2014	eIDAS
2015	Digital Single Market
2016	GDPR + NIS
2019	Cyber Security Act
2020	DSA + EUCSS
2021	AI Act
2022	DG Act + CR Act
2023	NIS2 Act

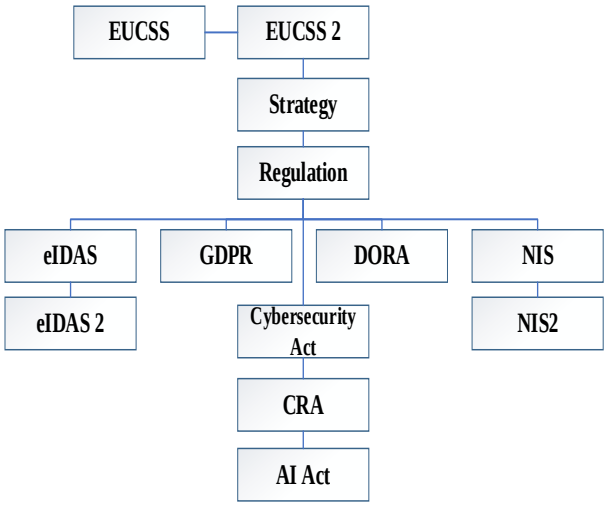


Fig. 1. EU Cyber Security Legislation – graphic display.

3. EVOLUTION FROM NIS TO NIS2

The NIS and NIS2 directives aim to strengthen the security of networks and information systems. In terms of the general scope of both directives, networks and information systems mean all electronic communication networks, equipment that enables digital data processing and data itself that is digitally processed (Article 4, paragraph 1).

The aim of the NIS2 Directive is to remove the shortcomings of the NIS and adapt it to the current needs. The NIS Directive applied to digital service providers (DSP) and operators of essential services (OES), in 7 (seven) different sectors including that of health, energy, transport, digital infrastructure and water supply. The NIS Directive left the discretionary right to the member states to identify the providers or operators of essential services, which introduces legal uncertainty, especially from the point of view of companies that have their operations in several countries. In order to overcome this shortcoming, the NIS2 Directive expands the scope of application by adding new sectors based on the degree of digitization and their significance for the economy and society itself. This means that NIS2 removes the distinction between DSP and OES by introducing two new categories (operators of essential services (OES) and important entities) and the size of a company that will be subject to different supervision. OES are companies that provide so-called critical services, that is, services that are essential for the functioning of society and the economy as indicated in Table 2. OES companies must comply with the NIS2 Directive regardless of their size. The group of important entities includes large or medium-sized enterprises (large enterprises includes companies that have over 250 employees or more than 50 million euros in annual revenues). Medium-sized enterprises are enterprises that have between 50 and 250 employees or an annual income of more than 10–50 million euros) that operate in the sectors listed in the following table. By introducing a definition of company size, the scope of the NIS2 Directive practically covers all medium and large enterprises in the selected sectors. Member States will also be able to include in the scope smaller entities but with a high security profile.

It should be emphasized that in comparison with NIS Directive, the proposed NIS2 Directive includes numerous examples of organizational and technical measures to improve the security of information systems. The NIS2 Directive, among other things, adds new requirements for 5 (five) primary areas (management, risk management, supervision, reporting and business continuity).

T a b l e 2

Description of OES and important entities

Operators of essential services (OES)	Important entities
Energy – electricity, heating and cooling, oil, gas, hydrogen	**Postal and courier services**
Transport – air, rail, water, road	**Waste management**
Banking & Financial market infrastructures	**Production, processing and distribution of food –** food businesses which are engaged in wholesale distribution and industrial production and processing
Health – Healthcare providers, laboratories, research and development of medicinal products, manufacturers of basic pharmaceutical products and preparations, manufacturers of medical devices considered to be critical during a public health emergency	**Manufacture, production and distribution of chemicals –** undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, and undertakings carrying out the production of articles from substances or mixtures
Drinking water – suppliers and distributors of water intended for human consumption	**Manufacturing** – manufacture of medical devices and in vitro diagnostic medical devices, manufacture of computer, electronic and optical products, manufacture of electrical equipment, manufacture of machinery and equipment, manufacture of motor vehicles, trailers and semi–trailers, manufacture of other transport equipment
Waste water – collectors, disposers, and treaters of urban, domestic, or industrial waste water	**Digital providers –** providers of online marketplaces, providers of online search engines, providers of social networking services platforms
Digital infrastructure – Internet exchange point providers; DNS service providers; TLD name registries; cloud computing service providers; data center service providers; content delivery network providers; trust service providers; providers of public electronic communications networks; providers of publicly available electronic communication service	**Research organizations**
ICT service management – (business–to–business) managed service providers (msps), managed security service providers (MSSPs)	
Public administration – public administration entities of central governments and at the regional level	
Space – operators of ground–based infrastructure owned, managed, and operated by member states or by private parties	

Management. – Management's task is to understand the NIS2 requirements and risk management efforts. Management has direct responsibility in the process of identifying and addressing cyber security risks and ensuring compliance with NIS2 requirements

Risk management. – Within the risk management process, the risk is identified, the probability and severity of the risk are taken into account as risk factors and the consequences of potential risks are predicted [17–18]. The NIS2 regulation, similar to NIS, provides discretion to regulated entities in setting their own rules and safeguards when it comes to the security of their systems. This type of regulation is known as "self-regulation" because it allows businesses to regulate themselves, while providing government authorities with the necessary control mechanisms to ensure that the procedures of regulated entities are appropriate and proportionate [19]. Hence the regulation mentioned by the NIS2 Directive can also be treated as a kind of metaregulation. Meta-regulation offers flexibility that is particularly important considering the complexity of information systems and different types of cyber attacks, but on the other hand it introduces certain difficulties when analyzing whether a regulated company fully

complies or does not fully comply with regulatory requirements. The shortcomings of meta-regulation can be overcome by proper oversight of all activities.

Supervision and fines. – Within the framework of the NIS Directive, the competent authorities of the member states had the opportunity to request information from OES about the current state of their information systems and findings from security audits. In addition, the competent authorities based on their own opinion could issue binding orders to those companies in order to strengthen their security protection. This approach assumed that supervisors have the necessary resources and skills to assess these risks. NIS2 increases surveillance as member states are required to establish investigative measures such as: regular audits, security surveillance of targeted system, inspections that can be conducted within the user's data centers or outside them, including random checks and security scans. In addition, for OES, member-countries should dedicate or appoint supervisor who will monitor the companies' compliance with risk management measures. In accordance with Article 30 of the NIS2 Directive, the powers of competent authorities are extended in the domain of supervision of important entities, which are similar in nature to the powers and measures imposed on OES. The main difference in the supervision of OES and important entities is that for the latter no supervisors are appointed to monitor companies' compliance with risk management measures. Perhaps more importantly, in accordance with Article 30 of the NIS2 Directive, important entities are subject to supervision only on the basis of evidence or indications of non-compliance. Such an approach can be an obstacle in the battle to increase the level of cyber security in the EU. High administrative fines provided by the NIS2 Directive can be treated as a bridge that can help to overcome these shortcomings [20]. Namely, the NIS2 Directive foresees relatively high administrative fines for OES (maximum of 10 million euros or up to 2% of the total annual turnover), while the fines for important entities amount to a maximum of 7 million euros or up to 1.4% of the annual turnover of the company. In order to ensure real liability in case of non-compliance, the NIS2 Directive provides provisions for the liability of natural persons in senior management positions in companies covered by the scope of the new NIS2 Directive. It is to be expected that administrative penalties for non-compliance can have a positive effect on companies [20].

Reporting. – When it comes to incident reporting, the right balance needs to be struck between the need for prompt reporting to avoid the potential spread of incidents and the need for detailed reporting that can help us to learn from each incident. NIS2 provides multiple ways of reporting incidents. Affected companies have a deadline of 24 hours from the moment they learn about the incident to give an early warning to the local CSIRT in order to request assistance, guidance or operational advice how to implement possible measures to mitigate the consequences of the incident. An early warning should be followed by a detailed incident report within 72 hours of becoming aware of the incident, while a final report should be submitted a month later.

Business continuity. – Organizations must be well prepared how to ensure business continuity in the event of a major cyber incident. This includes, for example, a recovery system, emergency procedures, the establishment of a crisis response team, and communication protocols in the event of a crisis.

4. HOW COMPANIES SHOULD ADAPT TO THE NIS2 REGULATION

Considering that the deadline for Member States to transpose NIS2 into national law is October 2024, companies subject to regulation by this directive must familiarize themselves with NIS2 recommendations.

Not all requirements defined in the NIS2 Directive apply equally to all businesses and organizations. The requirements of this directive vary depending on the size of the business and the role of that organization in society. In any case, there are a number of requirements that companies must meet in order to comply with the NIS2 Directive.

Asset inventory. – Asset inventory incorporates software tools and processes that enable record keeping of all hardware and software within an enterprise. In essence, it is a platform that will enable the automatic discovery of devices, applications and users, regardless whether they are mobile, static, IoT or in the cloud. Hardware asset management tool can configure and monitor the various relationships of every business-critical asset in company network. This may help during a change in the network infrastructure or during root cause analysis of a problem. Software Asset Management can help in keeping the track of company software assets and

licenses. Asset inventory is a basic prerequisite for building a mature and comprehensive security model, given that in this way all devices can be monitored and analyzed in terms of potential vectors of an attack.

Threat detection. – Threat detection is a process that includes timely identification of potential threats and creation of a response before the threat affect the business. When it comes to a company with multiple locations, an integrated and centralized solution is needed that will cover not only the headquarters but also the remote locations. There are several management systems that enable threat detection, such as SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), XDR (Extended Detection and Response).

SIEM is a solution that aggregates log data from multiple sources into one centralized platform. SIEM allows businesses to identify potential security threats and vulnerabilities before gaps can be exploited.

SOAR is a solution that identifies vulnerabilities based on vast amounts of collected SIEM data. SOAR uses automated workflows that enables mitigation without human intervention. Bearing in mind that SOAR is dependent on SIEM, these systems are often used in conjunction.

XDR is a cyber security solution that uses AI to detect anomalies in users behavior, as well as in the routers, servers, and endpoints of the network. XDR enables the automatic disconnection from a network of end devices that exhibit suspicious activity

Network segmentation. – Network segmentation is a security technique based on dividing a network into smaller, distinct subnets in order to define appropriate security controls at the level of each subnet eliminating a possibility for single point of failure. For example, if there is a cyber security breach in one subnet it will not affect the whole network. Network segmentation is usually done through a combination of firewalls, creation of Virtual Local networks (VLAN) or subnets. Firewalls are deployed inside the network to create internal zones that divide functional areas from one another. A VLAN is a way of logically separating a group of computers into a separate network. This means they will only communicate with each other and not with any other devices connected to the same physical network. Subnets use IP addresses to create a logical partition of an IP network into multiple, smaller network segments.

Policies and procedures for the use of encryption. – Increasing the use of encryption is one of the main goals of NIS2. Of course, a large part of the communication is already encrypted using protocols such as ssh and https when it comes to computer-computer or computer-server communication or by using IPSEC, MPLS VPN or SDWAN type of services when it comes to security connecting one or more remote locations.

Security procedures for data access. – Security procedures for data access should apply not only to employees within the company, but they should also cover the relationship between the company and the direct supplier. There are several types of management systems that can enhance the security procedures for data access. In this paper we will focus on two, maybe the most important systems: PAM (Privileged Access Management) solutions and MFA (Multi-Factor Authentication). PAM is a solution that helps protect organizations against cyber threats by making sure that people have only the necessary levels of access to do their jobs. This solution is exceptionally important when the company collaborates with their supply chain in a digital manner. MFA is a login process that requires users besides the password to enter more information like a code sent to their email, SMS, scanning a fingerprint, or simply answer a secret question.

Business continuity plan. – A plan for managing business operations should be created in a way that will guarantee access to IT systems and their operational functions during and after a security incident. It should consist of at least three steps. As part of the first step, the critical on-premise and cloud infrastructure should be scanned. The second step is prioritizing critical systems, while the third step is introducing regular backups and testing the backups and business continuity process to ensures that data recovery is possible in the event of a real crisis.

Risk management and periodic risk assessments. – Risk assessment is vital for any organization, but risk assessment is not a one-time job. New vulnerabilities in the systems may appear due to changes in network configuration and business processes or due to emerging new threats in the ever-changing cyber security landscape. The risk assessment consists of two basic parts. The first part refers to the Security Review & Gap Analysis whose task is to generate a complete and comprehensive process for defining security risk strategies based upon your objectives, security posture and status. The

second part refers to periodically performing network vulnerability testing. Vulnerability assessment and penetration testing are the most common methods for assessing the security risk of systems [21] (Weber et al., 2017). Many people believe that vulnerability assessment and penetration testing are two same terms, but actually these two terminologies differ to some extent. Vulnerability assessment is defined as the automatic identification of system weaknesses, while penetration testing mainly refers to a form of stress testing that detects weaknesses in networks and sets measures to overcome these vulnerabilities in the network

Incident response and reporting. – The NIS2 Directive demands timely and appropriate reporting, so regulated companies need to know how to respond before an incident occurs: how to collect warning information, how to track incidents, how to report actual incidents and to whom. The threat-detection solution described above should be able to help operations and security teams to easily comply with NIS2 reporting prerequisites.

Cyber security training and a practice for basic computer hygiene. – Given that the majority of successful cyber attacks occur as a result of targeted fishing campaigns, NIS2 requires organizations to provide training to their management and employees to deepen their cyber security knowledge. Within the cyber security framework, various trainings can be included such as: awareness trainings, continuous training program and courses appropriate to the employee level in the organization, type of work, and exposure to security threats.

5. N. MACEDONIA – CYBER SECURITY LEGAL FRAMEWORK, ADOPTION OF NIS2, CHALLENGES AND RECOMMENDATIONS

N. Macedonia is slowly but steadily working towards developing a secure cyber environment. The Government of N. Macedonia aims to improve its ability to protect infrastructure such as energy, telecommunications, and e-services and ensure that systems and structures are in place to meet the future requirements of international allies such as the European Union and NATO. The first significant step was taken in 2018 when the Cyber Security Strategy (2018–2022) including an Action Plan was developed (available at www.mioa.gov.mk). Through the identification of main stakeholders and through the identification of goals, measures, and activities, the strategy and the action plan aim was focused on fostering the development of a safe, secure, reliable and resilient digital environment in the country.

In 2021, N. Macedonia adopted the National ICT strategy (2021–2025) (available at www.mioa.gov.mk). The strategy had six pillars:

- Interoperability and government infrastructure;
- Centralization of ICT and e-government services;
- Improved people digital skills;
- R&D (research & development);
- Data protection;
- Digital services.

In 2021, N. Macedonia signed a memorandum of understanding with NATO which aims to facilitate the exchange of information and best practices when it comes to cyber threats. Ministry of Defense in accordance with the National Cyber Security Strategy, the EU Strategy and NATO standards developed the Strategy for Cyber Defense. This strategy aims to provide improved protection of national interests by developing and strengthening local capabilities to monitor and reduce the impact of cyber security risks.

In addition to the adoption of the National Cyber Security Strategy (2018–2022), a series of other documents relevant to cyber security in the country were adopted. For example, with the adoption of the Law for Electronic Communications, a National Computer Incident Response Center (MKD-CIRT) was established as a separate unit of the Agency for Electronic Communication. MKD-CIRT, similar to the CIRTs in the EU member-states, aims to raise the protection of network and information security to a higher level.

The Law on Personal Data Protection was originally adopted in 2005. As a result of the need to harmonize this law with the EU Regulation regarding the Protection of Personal Data (GDPR), a new Law on Personal Data was adopted in February 2020. From August 24, 2021, the Law on Personal Data is fully in force.

Currently, there are a number of documents related to cyber security that are under development. The Ministry of Defense is working on Law on Critical Infrastructure, while the Ministry of Information Society is working on new National ICT Strategy (2023–2030) and new National Cyber Security Strategy (2023–2030). In parallel Ministry of

Information Society is also working on preparing the Law on Security of Network and information Systems, and Digital Transformation.

The aim of the Law on Critical Infrastructure is to define critical physical infrastructure sectors that must be protected. This law identified 9 (nine) critical sectors:

- Energy (production, including dams, mining, storage, transportation of energy, and energy distribution, etc.).
- Transport (road, rail, air and water traffic).
- Banking systems and infrastructure of the financial markets.
- Health (health care, production, trade and control over medicines).
- Water supply (water supply and drainage systems).
- Food (food production and supply).
- Production, storage and transportation of dangerous substances (chemical, biological, radiological and nuclear materials).
- Public services (ensuring public order and peace, protection and rescue, emergency medical assistance).
- Digital infrastructure, communication and information technologies (electronic communications, data transfer, information devices and installations, audio and audiovisual media services, etc.).

The owners/operators of critical infrastructure are obliged to create and update the security plan or the equivalent document in accordance with the applicable regulations and are obliged to establish an internal crisis management and crisis communication system for all matters important for the operation of the critical infrastructure.

The new National ICT Strategy 2023–2030 is focused to set a clear roadmap for better digitization of society, which directly affects the quality of life of citizens. The strategy is based on 4 basic pillars:

Pillar 1: Gigabit connectivity and ICT infrastructure). – This pillar consists of three strategic objectives: provision of gigabit connectivity to public institutions, development of Government ICT infrastructure and development of National educational ICT infrastructure.

Pillar 2: Developing digital skills. – This pillar covers the implementation of training programs for development of ICT skills.

Pillar 3: Digital management, with enhanced support for digitization of businesses. – Digital governance consists on development of three strategic objectives: e-services, digital identity, and cyber security.

Pillar 4: ICT enablers and digital innovation. – This pillar consists of three strategic objectives: horizontal platform, open data, promotion of innovation and digitization of SMEs (small and medium enterprises).

The new National Cyber Security Strategy (2023–2030) is prepared taking into account ENISA guidelines and tools for the development of national cyber strategies. This strategy lay on 5 pillars:

- Pillar 1: Building clear and robust cyber security governance structure;
- Pillar 2: Security and resilience of networks, information and communication systems;
- Pillar 3: A society resilient to cyber threats;
- Pillar 4: Minimizing the impact of incidents in cyberspace;
- Pillar 5: National and international cooperation.

Within Pillar 1, the establishment of a National Council for Cyber Security and creation of a SPOC (Single Point of Contact) is foreseen in order to ensure efficient cross-border cooperation with the relevant authorities of other countries, EU member states, European Commission, ENISA and NATO. Within the framework of Pillar 1, the creation of a unique and comprehensive legal framework for cyber security management is also envisaged, through the adoption of a new law, in line with the NIS2 Directive (Directive – EU 2022/2555). Within Pillar 2, in accordance with the NIS2 Directive, high and other critical sectors are defined in the way they correspond with operators of essential services (OES) and Important entities from NIS2.

Another significant document in preparation related to cyber security is the Law on Security of Network and Information Systems, and Digital Transformation. This law aims to provide legal framework that will be in accordance with the NIS2 Directive.

Enacting the appropriate legislation is a step in the right direction when it comes to setting a platform for the upliftment of Cyber Security. In that regard, N. Macedonia is on the right path. However, there are a lot of challenges for Government, infrastructure operators and the private sector that needs

to be addressed. Below are some of our recommendations:

Finalization of strategies related to cyber security: Adoption of National ICT Strategy (2023–2030) and National Cyber Security Strategy (2023–2030).

Effective legal framework: Finalizing laws that are currently in the stage of public debate, such as the Law on Security of Network and Information Systems, and Digital Transformation, and Law on Critical Infrastructure.

Harmonized policies: By adopting the National ICT Strategy, National Cyber Security Strategy and series of laws related to cyber security, the government and key institutions should prevent overlapping of legal provisions by clarifying the roles of each of the institutions separately.

NIS2 compliance: The government should prepare recommendations for the entities that will be regulated by NIS2 in terms of recommended management systems for Asset Inventory, Threat Detection, Encryption, Security procedures for data access, etc. in order to better monitor the compliance with NIS2 Directive.

Education: There is a shortage of qualified cyber security personnel due to an outdated education system and teaching methodologies, non-standardized cyber security job descriptions and qualifications, and a significant brain drain to other countries. The government and educational institutions must start working on the production of qualified personnel.

Public awareness campaign: The government in cooperation with the private sector and civil initiatives should invest more in campaigns aimed at raising awareness of the importance of cyber security. In this way, people would be aware of the risks they may face when using the Internet without adequate protection.

Regional cooperation: Considering that the majority of cyber attacks originate outside the Balkan region, the Government should have a more proactive approach in order to have greater cooperation with other countries from the Western Balkans.

International cooperation: The institutions in N. Macedonia should intensify their efforts to participate in cyber security initiatives and projects, as well as the development of regional, European and international partnerships. N. Macedonia as a country does not have the capacity to independently protect itself from cyber attacks, therefore wider coordination and cooperation is essential.

6. CONCLUSION

Digitization is essential for developing a functional, efficient and modern government and society. The Macedonian government is continuously increasing the number of digital services. The rapid adoption of digital technologies exponentially increases the risk of successful cyber attacks. Developing countries such as N. Macedonia are less resistant to cyber attacks especially when these attacks are aimed at critical infrastructure.

Although N. Macedonia has a solid legal system, it needs to be upgraded by adopting the Cyber Security Strategies (ICT Strategy (2023–2030) and National Cyber Security Strategy) and by bringing into force the Law on Critical Infrastructure and the Law on Security of Network and Information Systems, and Law on Digital Transformation.

Different types of cyber attacks show that N. Macedonia should work even more on creation of an effective response to such cyber attacks threats in order better to protect the national security. Therefore, apart from the completion of the previously mentioned legislation, the focus must be placed on education, harmonized policies, public awareness campaign, regional and international cooperation.

REFERENCES

[1] Statista (2024): Overview. Accessed 27.02.2024. https://www.statista.com/topics/4123/internet-of-things-iot-in-europe/#topic

[2] BIRN (2021): Online intimidation: Controlling the Narrative in Western Balkans.

[3] Taddeo, M. (2013): Cyber security and individual rights. striking the right balance. *Philosophy & Technology*, **26** (4), pp. 353–356.

[4] Gordon, L. A., Loeb, M. P., Lucyshyn, W. (2020): Cybersecurity investments in the private sector: The role of Governments. *Georgetown Journal of International Affairs*, pp. 79–88. Accessed May 17, 2021. http://www.jstor.org/stable/43773651.

[5] Michels, J. D., Walden, I. (2020): Beyond "Complacency and Panic": Will the NIS Directive improve the cybersecurity of critical national infrastructure? *European Law Review*, pp. 25–47.

[6] Clark-Ginsberg, A., Slayton, R. (2018): Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science and Public Policy*, **46** (3), pp. 339–346.

[7] *EU Cybersecurity Strategy*, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

[8] *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. https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[9] *Directive (EU) 2022/2555* of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[10] *Regulation (EU) 2016/679* of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

[11] *Regulation (EU) 2022/2065* of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065

[12] *Regulation (EU) 2022/868* of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868

[13] *Regulation (EU) No 910/2014* of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=uriserv%3A OJ.L_.2014.257.01.0073.01.ENG

[14] *Directive (EU) 2015/2366* of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri =celex%3A32015L2366

[15] *Regulation (EU) 2022/2554* of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[16] *Regulation (EU) 2019/881* of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). https://eur-lex.europa.eu/eli/reg/2019/881/oj

[17] Gellert, R. (2020): *The risk-based approach to data protection*. Oxford University Press.

[18] Lin, W. C., Saebeler, D. (2019): Risk-based v. compliance-based utility cybersecurity – A false dichotomy? *Energy Law Journal* **40** (2), pp. 243–282.

[19] Parker, C. (2002): *The Open Corporation: Effective Self-regulation and Democracy*. Cambridge University Press.

[20] Voss, W., Gregory and Bouthinon-Dumas, H. (2021): EU general data protection regulation sanctions in theory and in practice. *Santa Clara High Tech. Law Journal* **37** (1), pp. 1–97.

[21] Weber, R; H., Staiger, D. (2017): *Transatlantic Data Protection in Practice*. Springer.

Journal of Electrical Engineering and Information Technologies, Vol. **9,** No. 1, pp. 63–70 (2024)
Article 220
In print: ISSN 2545–4250
Received: December 25, 2023
On line: ISSN 2545–4269
Accepted: April 15, 2024
UDC: 004.382.7'142.6:004.93'1]:621.396.96
https://doi.org/10.51466/JEEIT2491220063m

Original scientific paper

DIGITAL DEVELOPMENT BOARD FOR SHORT RANGE OBJECT DETECTION WITH STEGANOGRAPHIC DATA HIDING TECHNIQUES

Rexhep Mustafovski, Aleksandar Risteski, Tomislav Šuminoski

Faculty of Electrical Engineering and Information Technologies,
Ss. Cyril and Methodius University in Skopje,
Karpoš 2 bb, 1000 Skopje, R. N. Macedonia
tomish@feit.ukim.edu.mk

A b s t r a c t: This scientific paper discusses the application of single-board computers in performing various projects focusing on the practical development of a radar system for detecting objects at short distances using the digital development electronic board Arduino Mega 2560, that contribute to the development of electronic technology, microcomputers and microprocessors and their application for educational purposes. An overview of various literary sources related to the development of digital electronics, microprocessors, digital forensics as an important scientific discipline within the security of sharing various information and their application during the development of various educational projects has been used. Additionally, various methods and techniques used in steganography are illustrated, a study of the implementation of those techniques, and a demonstration of the implementation process of one of the steganography techniques using the QuickStego steganography tool. The development of the radar system for the detection of objects at short distances was carried out by programming the ultrasonic radar system using the tools Arduino IDE, Processing PDE, Matlab and Simulink, which offer support for the Arduino hardware.

Key words: microprocessors; Arduino Mega 2560; QuickStego; Arduino IDE; processing PDE

ДИГИТАЛНА РАЗВОЈНА ЕЛЕКТРОНСКА ПЛОЧА ЗА ДЕТЕКЦИЈА НА ОБЈЕКТИ НА КРАТКИ РАСТОЈАНИЈА СО СТЕГАНОГРАФСКИ ТЕХНИКИ ЗА КРИЕЊЕ НА ПОДАТОЦИ

А п с т р а к т: Во овој научен труд се разгледува примената на компјутерите со една плоча при изведување различни проекти, фокусирајќи се на практичната изработка на радарски систем за детекција на објекти на кратки растојанија со помош на дигиталната развојна електронска плоча Arduino Mega 2560, што придонесува за развојот на електронската технологија, микрокомпјутерите и микропроцесорите и нивната примена за образовни цели. Користени се и даден е преглед на различни литературни извори кои се однесуваат на развојот на дигиталната електроника, микропроцесори, дигитална форензика како важна научна дисциплина во рамките на безбедноста на споделувањето на различни информации и нивната примена во текот на изработка на различни образовни проекти. Дополнително се илустрирани различни методи и техники кои се користат во стеганографијата, проучување на имплементацијата на тие техники и прикажување на процесот на имплементација на една од техниките за стеганографија со користење на стеганографската алатка QuickStego. Изработката на радарскиот систем за детекција на објекти на кратки растојанија е извршена со програмирање на ултразвучниот радарски систем со помош на алатките Arduino IDE, Processing PDE, Matlab и Simulink, кои нудат поддршка за хардверот Arduino.

Клучни зборови: микропроцесори; Arduino Mega 2560; QuickStego; Arduino IDE; processing PDE

1. INTRODUCTION

The topic of this scientific paper has a wide application in the field of digital electronics and digital forensics as important scientific branches in the digital world. At the same time within the framework of programming and the use of algorithms which are key elements in the course of the development of the

practical part within the scientific paper, i.e. the creation of a ultrasonic radar system for the detection of objects at short distances using the Arduino Mega 2560 digital development electronic board. The scientific paper shows the importance of the application of single-board computers in various educational processes and areas that are key factors for development and scientifically advancements in technology today. Digital forensics is also considered as a scientific discipline for collecting, storing, and analyzing information and data that are transmitted or stored in digital form and represent a certain importance for an organization or an individual that proves a certain veracity of the information and data itself. Through various literary sources are explained the importance of information security in order to carry out communication between the users themselves in a protected form. The scientific paper itself presents certain methods and techniques used in steganography to hide information and data in various digital formats using the QuickStego steganographic tool that allows all information and data to be transmitted safely without compromising their security, study of the same techniques and a practical presentation of the implementation process of the steganographic technique itself. Through the practical development of the Ultrasonic Radar System for the detection of objects at short distances (furthermore: URSAD), in this scientific paper is showed the way to successfully connect the Arduino Mega 2560 digital development electronic board (programmed with the Simulink simulation tool or with the Arduino IDE tool) with a personal computer using a program made with the Processing PDE software. It allows to finally display on the computer screen the presence of a certain object detected by the short-range object detection ultrasonic radar system. The integration of the Arduino Mega 2560 digital development electronic board with the digital electronic platform, i.e., the integrated development environment Arduino IDE and the processing development environment Processing PDE, which enables the programming of the Arduino Mega 2560 digital development electronic board and display on the computer screen, is also shown.

Further it’s demonstrated the practical implementation of the steganographic technique for hiding information in an image with the received data from the serial port of the Arduino IDE tool for the distance and angle for the detected object from the short-range object detection ultrasonic radar system to enable that information securely to be sent over the communication channel [15].

2. SINGLE BOARD COMPUTERS

A single-board computer is a device or digital component that contains only the most necessary circuitry needed to operate as a machine. These boards, or single-board computers, are often shipped without cases and other accessories in order to keep the selling price low. A single-board computer is also called a digital development electronic board or a development board, because they can be programmed and connected to various digital electronic platforms that allow the construction of various systems or devices that develop the scientific branch itself as a scientific discipline in today's digital science. The most important component, the heart of a single-board computer, is the microprocessor. A microprocessor is a unit that has several General-Purpose Input/Output (GPIO) ports that can be used for different digital applications, platforms, and can be programmed to work in a certain way. There are many manufacturers of microprocessors available in the market and each manufacturer and brand has its own main purpose and purpose with which they differ in selling price, capabilities, features that offer users opportunities to use them for making and experimenting with various projects and scientific experiments from different disciplines and fields [6, 7, 8, 9, 15].

Today's single-board computers are supported by a large Internet community around the world, where hobbyists and professionals share projects, scientific experiments, scientific journals and papers, and help each other solve various problems encountered during their construction, projects or scientific experiments. The large community is also an important factor when it comes to educational purpose. Information and data are easy and most likely someone has already done a similar thing, which can be a source of inspiration. Very often the source codes are provided (open source), which makes it easy for anyone interested to start a project or a particular experiment.

Depending on the application, different board specifications are required. Some boards, or digital development boards, are designed as multimedia players and therefore need a microprocessor that can handle video and audio acceleration. Another popular single board computer is the Arduino digital development board. It was started as a school project with the main goal of developing a cheap solution that could be learning programming and electronics. This approach was quickly liked by amateurs and researchers who found large areas of use,

which contributed to the development of the community around the platform. The Arduino digital development electronic board is designed to be programmed within their own integrated development environment (IDE – Integrated Development Environment) and uses the C^{++} programming language as a simple learning language for students in the educational process. It also has the ability to expand with compatible shields. A shield is a complete add-on circuit that can be placed directly on the Arduino board and can be programmed and used with various applications. Such an example is a shield for network communication between controllers (CAN BUS – Controller Area Network) which enables the Arduino protocol and the Servo Motor Shield which makes the Arduino capable of controlling servo motors. Arduino is one of the most prominent platforms on the market and an open access board, which means that anyone can buy the parts separately, download the schematic and build it at home. Since the digital development circuit board is open source, there are many different variants of the main board. The Arduino Nano-digital development board is the smallest board, which has very low power consumption and can be used for applications that do not require a lot of expandability. The Arduino Uno-digital development board is one popular development board in the Arduino family of digital development boards. There are several different types of integrated protocols, but there is no video output as a standard option. It is often used as a prototype for projects and products before the board is scaled down and adapted to the application [2, 3, 9, 15].

The Arduino Corporation initiated a collaboration with Intel and developed a new board, that is, a digital electronic development board called the Arduino Galileo. The Arduino Galileo digital development board has been launched as an Internet of Things (IoT) development board and has a more powerful processor than its predecessor and also has the ability to run a Linux operating system. It has the same physical form factor as the Arduino Uno-digital development board, which means it can be used with most existing shields and code with minor modifications [9, 12, 15, 16].

The Arduino digital development circuit board was a turning point for the concept of single-board computers as we know them today. It has been proven useful in many applications and has a lot of support from the Internet community. Thanks to the open source, various versions have been developed and extended to different application areas. There are several development boards available in the market with different specifications and vendors. This has also led microprocessor manufacturers to add more features to the processor itself [9, 10, 11, 15, 17].

3. ARDUINO MEGA 2560 DIGITAL DEVELOPMENT ELECTRONIC BOARD

Arduino Mega 2560 is shown in Figure 1 and it represents a platform based on the Atmel ATMega 2560 microcontroller. In addition to the microcontroller, it also contains a number of elements and components necessary for its proper operation. Programming and communication with the computer is done using a USB port. It is compatible with a number of other Arduino boards and with the Duemilanove and Diecimila platforms. The Arduino Mega 2560 digital development electronic board, unlike other Arduino boards, has more inputs to which sensors can be connected. The technical specifications of the Arduino Mega 2560 digital development electronic board are shown in Table 1 [4, 13, 15].

Fig. 1. Arduino Mega 2560 single board computer [2, 15, 18].

The operating voltage that can enable this microcontroller through a pin, as with most Arduino boards, is 5 V. The limit value of the input voltage has a range from 6 to 20 V, and the recommended voltage at which this microcontroller works is from 7 to 12 V. There, are 54 digital input/output pins, 14 of which support pulse-width modulation. It also has 16 analog inputs and a 16 MHz crystal oscillator. It can be powered by a USB port or an external source [3, 4, 13, 15].

4. DIGITAL ELECTRONIC COMPONENTS AND PARTS FOR THE PRACTICAL PART

In this section are shown all the digital electronic components and parts that were used for the practical part of URSAD for object detection in short range (see Table 2).

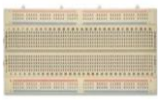
Table 1

Technical specifications of the digital single board computer Arduino Mega 2560 [14, 15, 18]

Microcontroller	*ATmega2560*
Operating voltage	5 V
Recommended input voltage	7 – 12 V
Input voltage limit values	6 – 20 V
Digital input/output pins	54 (15 of which provide PWM output)
Analog input pin	16
DC input/output pin	20 mA
DC for 3.3 V pin	50 mA
Polarity of external adapter	The middle part is positive
Number of digital outputs	14 (6 of which have PWM capability)
Number of analog outputs	6
Input/output amperage	40 mA
Flash memory	256 kB of which 8 kB used by the bootloader
SRAM	8 kB
EEPROM	4 kB
LED_BUILTIN	13
Operating frequency	16 MHz
Dimensions	101,52 x 53,3 mm
Mass	37 g

Table 2

Used digital electronic components and parts for the practical part [15]

Components	Name of components
	Arduino Mega 2560
	USB cable
	Breadboard
	Jumping Wires
	Light-emitting diode (LED)
	Servo Motor
	Ultrasonic Sensor HC-SR04

5. ALGORITHMS FOR FUNCTIONS IN THE INTEGRATED DEVELOPMENT ENVIRONMENT

The code in the Arduino IDE integrated development environment is done with a combination of the C and C^{++} programming languages. As already mentioned earlier in this paper, the code of the integrated development environment consists of two main functions void setup() and void loop() [1, 15, 18, 19, 20].

In the Figure 2 is depicted the algorithm for the functionality of the servo motor, which allows to rotate from 0 to 180 degrees and with that the ultrasonic sensor can detect the objects in the range of 40 cm by appearing the detected objects in the screen of the laptop. In the Figure 3 is shown the algorithm for the function calculateDistance that is used in the code, which precisely gives the mathematical equation of the way of measuring the distance of the object.

6. ALGORITHMS FOR FUNCTIONS IN THE PROCESSING DEVELOPMENT ENVIRONMENT

Figure 4 illustrates the algorithm written in Processing code within the Processing Development Environment. This code facilitates the creation of the URSAD display and enables the visualization of potential detected objects on the PC screen.

Furthermore, in the Figure 5 is shown the model development in Simulink, which practically allows to integrate the digital electronic board Arduino Mega 2560 with the Processing Development Environment (Processing PDE).

Since a lot of things happen in the background, the algorithm for the void setup() and void loop() functions will be presented. First we have the definition of variables and constants, then the value $i = 15$ is sent to the loop that checks if it is less than or equal to the value 165, if the answer is yes then that value is sent to the servo motor where there is a short stop process of 30 microseconds and those values along with the distance are sent to the computer program and finally the value of i will increase by one more value and thus this cycle will repeat where the servo motor turns from 15 to 165°, if the answer is no then the value of $i = 165$ where the condition is checked if it is greater than the number 15, if the answer is no then that value is sent to the servo motor where there is a short stop process of 30 microseconds and those values along with the distance is

sent to the computer program and finally the value of *i* will decrease by one less value and thus this cycle will repeat where the servo motor turns from 165 to 15°, if the answer is no then we go back to the previous function from the algorithm. These two functions of the Arduino code are shown with an algorithm in Figure 2.

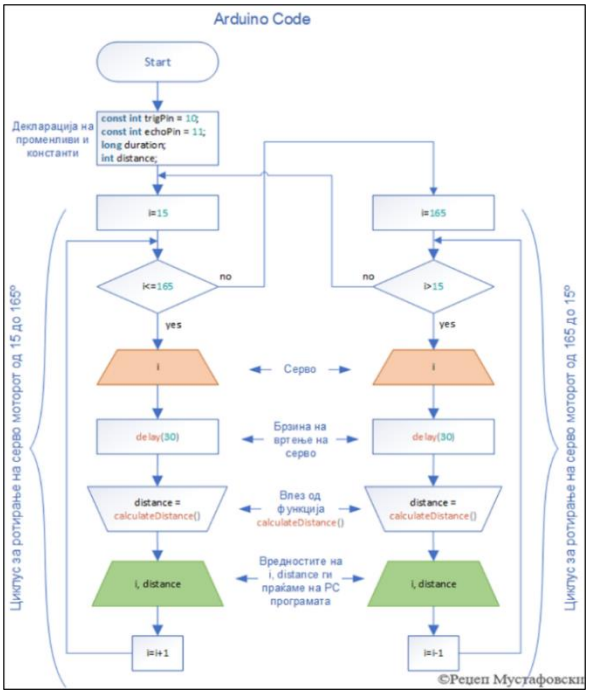


Fig. 2. Algorithm for void setup() and void loop() functions [15]

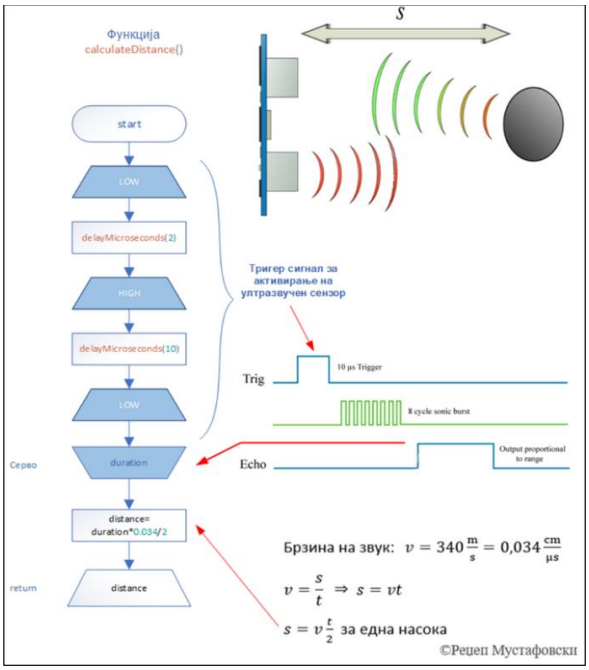


Fig. 3. Algorithm for the calculateDistance process [15]

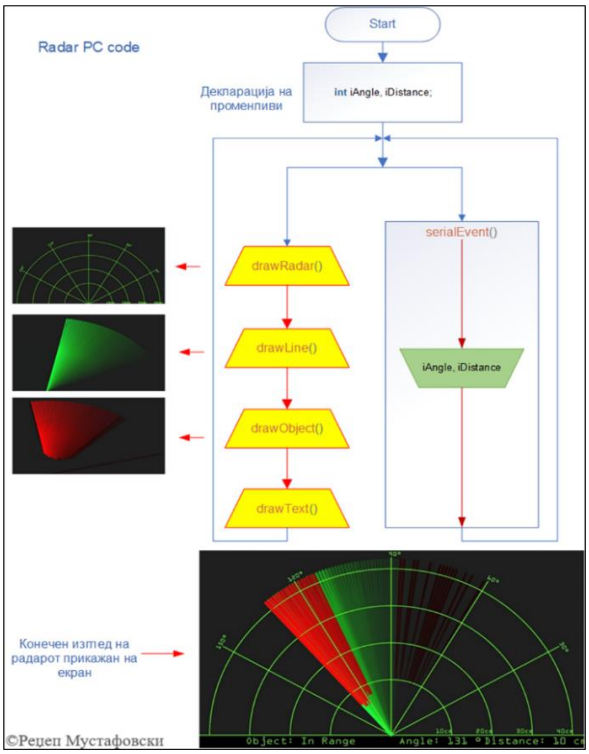


Fig. 4. Algorithm for Processing's code [15]

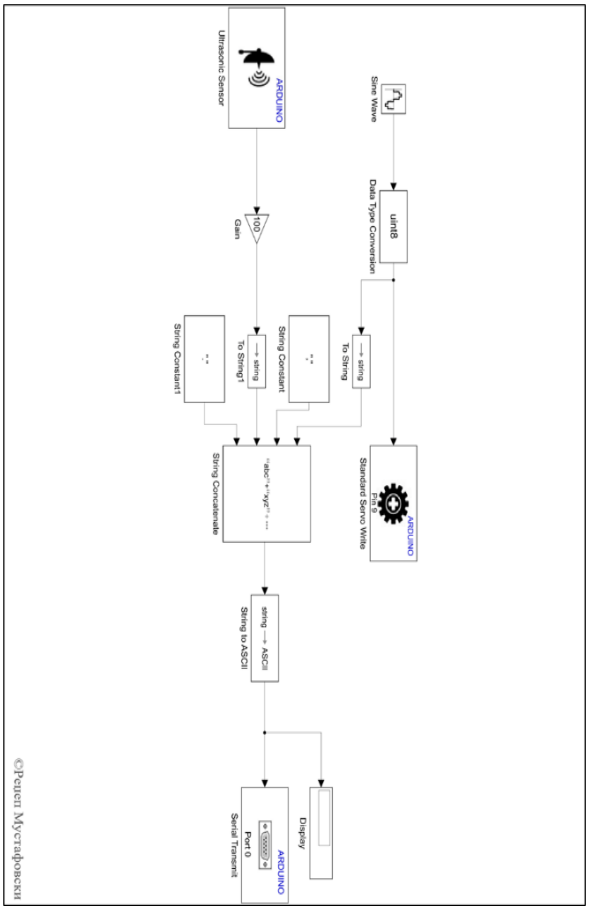


Fig. 5. Appearance of the model in the Simulink simulation tool [15]

As an additional process that is mentioned in the explanation of the void loop() and void setup() functions, and is very important, is the process for calculating the distance, i.e., calculateDistance(). This process is mainly performed by the ultrasonic sensor. A trigPin is given as an output value, if the emitted signal is not rejected it means that we have no target, and then a new signal is emitted again.

When the signal is rejected, then echoPin is at logic zero. The distance calculation process is shown by the equation distance = duration*0.034/2, where the distance for each object can be different. The complete distance calculation process is shown by the algorithm in image no. 3.

7. PRACTICAL APPEARANCE AND CONNECTION OF THE URSAD

From the information presented thus far, we've developed a conceptual understanding of the ultrasonic radar's potential appearance and functionality. This section will specifically show the appearance of the URSAD and its function through pictures.

Through the graphic display shown in Figure 6, a visual representation of what the URSAD looks like in reality is obtained. The difference in reality is that the ultrasonic sensor itself is attached to the servo motor.

The Figure 6 presents the connection of different colored wires, usually the black wire is used to connect the common end or the minus, the red wire is used to connect the positive pole of the power supply, while the rest of the wires can be chosen as desired. What is important when connecting the rest of the parts and the various wires is visibility during the connection. Transparency in connectivity allows for easier inspection of connected elements [15].

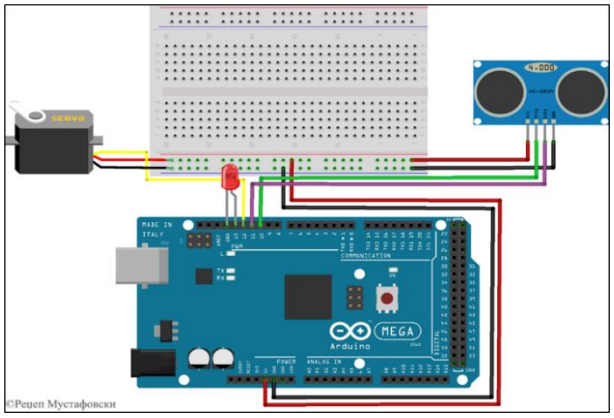


Fig. 6. Connecting the components of the URSAD [15]

The Processing program created in the processing development environment plots the URSAD surface based on the information and display of the detected target. The developed URSAD for the detection of objects at short distances as part of this paper in our laboratory is shown in Figure 7.

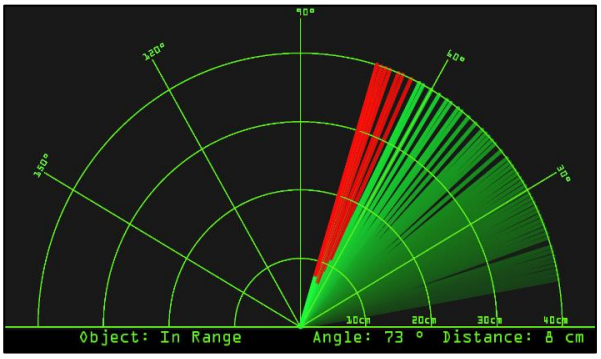


Fig. 7. The realistic appearance of the URSAD system for detecting objects at short distances [15]

8. PRACTICAL DEMONSTRATION OF HOW TO HIDE INFORMATION IN AN IMAGE USING THE QUICKSTEGO TOOL

In the following section with practical demonstration are explained the steps of how-to code and decode the information using the QuickStego tool.

a) *Coding or encryption of information*

In this part of the paper are explained the following steps of coding or encryption of information:

1) Open QuickStego tool to implement image steganography. Now click on the "Open image" button to open the image [5, 15].

2) To select the cover image, click any image that will act as our cover image to implement steganography to hide our secret data. In our case, the cover image marked as a test image will be selected, on which text will be hidden [5, 15].

3) After selecting the cover image, it is loaded into QuickStego [5, 15].

4) Now we can write our secret message on the cover image displayed on the tool on which the steganography will be performed.

This message is written in the black message box on the right side of the cover image. The data, i.e., the information that will be hidden in the image, then will be taken from the output of the serial port of the integrated development environment Arduino IDE for the angle and distance of the object detected

by the URSAD system [5], [15]. Figure 8 displays the results regarding the detected angle and distance of the object as captured by the ultrasonic sensor.

5) Click the “Hide text” button to hide the text and save it on the image, otherwise it will not be saved. Then the text message is hidden in the image as shown in Figure 9 [5, 15].

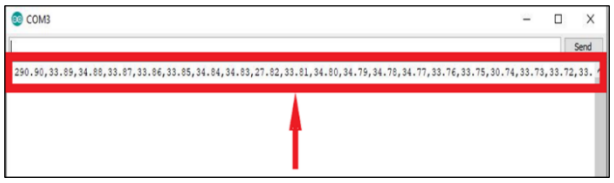


Fig. 8. Angle and distance data of the detected object from the URSAD system [15]

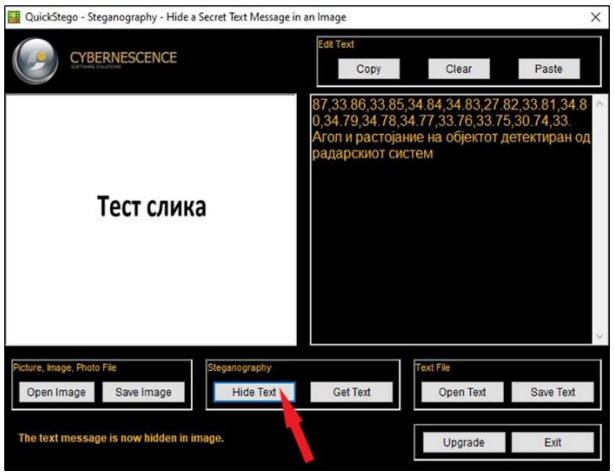


Fig. 9. Hiding the secret message in the cover image [15]

6) Clicking the "Save image" button to save the image allows QuickStego users to select the location where the image containing the hidden data will be saved [5, 15].

This is the file that when transferred will appear to be any normal image, but actually has some secret data hidden inside the image itself.

b) *Decoding or decryption of information*

1) Open the QuickStego tool and then click "Open image" to open an image [5, 15].

2) On the picture select the header or cover image that was received from the sender [5, 15].

3) The selected cover image is now opened in QuickStego tool which will display the hidden text message in black screen [5, 15].

4) In case the text is not displayed, it can be obtained by clicking the "Get text" button to display the hidden text from the title image [5, 15].

9. FUTURE WORK

In order to enhance the Arduino Mega 2560 radar system for short-distance object detection, we should consider these future steps [19, 15]:

1. Enhance Detection Accuracy: Refine radar sensitivity and signal processing for more accurate object detection.

2. Expand Object Recognition: Develop algorithms for recognizing specific objects detected by the radar.

3. Optimize Hardware Setup: Streamline connections and components for better efficiency and reduced size if applicable.

4. Implement Range Adjustment: Enable adjustable range settings for versatile detection capabilities.

5. Enable Remote Monitoring: Investigate ways to monitor detections remotely, possibly via wireless connectivity.

6. Develop User Interface: Design a user-friendly interface for intuitive system control and data visualization.

7. Test and Validate: Conduct thorough testing under various conditions to validate and refine the system's performance.

10. CONCLUSION

In this paper, we present several achievements with the application of digital development electronic boards or single board computers. Their application in many other different scientific fields and branches or combination with new codes or models allows controlling, operating and giving instructions to all digital development electronic boards and digital components to build different systems with specific functions and capabilities.

In the overall work of this scientific paper, the flexibility, characteristics and possibilities of digital development electronic boards, their open code and their application for various scientific fields, through which their unlimited connection and combination with other digital development electronic boards, components, software and computers are shown. These digital development electronic boards, i.e., single-board computers, have a price that is accessible to everyone, offer advanced features, while being simple and can be used by students in the educational process, for various other scientific projects and experiments in other scientific fields and disciplines. Digital electronic boards can be used in the educational process and the study

process, which are an important factor for the development of education itself, and can also be used in the industry to carry out various processes with which they save certain human and time resources. Steganography, a subset of digital forensics, employs diverse methods to securely transmit crucial information, playing a pivotal role in technology's advancement for safe communication and data transfer.

The URSAD system detects nearby objects and connects with the Arduino Mega 2560 board through the Arduino IDE and Processing PDE. The configuration shows cases for object detection on a computer screen by utilizing data gathered from the Arduino Mega 2560 hardware, summarizing the accomplishment achieved with the short-range ultrasonic radar system for object detection. It was also shown how to connect the Arduino Mega 2560 digital development board with the Simulink simulation tool.

Practical implementation of the steganographic technique for hiding information in an image using the steganographic tool QuickStego with the data obtained from the serial port of the Arduino IDE tool for distance and angle for the detected object from the short-range object detection URSAD system was also shown in practice. Moreover, the framework presented here enables the information to be sent securely over the communication channel [15]. Also, the URSAD system demonstrates promising potential in short-range object detection, showcasing a practical fusion of hardware and software capabilities to enable precise and efficient identification of nearby objects, marking a significant stride in innovative technological advancements.

In the near future, radar systems for detecting nearby objects will see improvements through various strategic advancements focused on refining methods and system design. These efforts aim to achieve better precision, superior outcomes, and overall system advancement.

REFERENCES

[1] Ставрова, А. (2020): *Дигитални електронски платформи со отворен код*. Дипломска работа, Воена академија „Генерал Михаило Апостолски“, Скопје.

[2] Dino, C. (2012): *Mobilni robot na gusjenični pogon*. Diplomski rad, Fakultet strojarstva i brodogradnje, Zagreb.

[3] Luka, C. (2014): *Bespilotna brodica sa vlastitim propulzijskim sustavom i upravljanjem*. Diplomski rad, Fakultet strojanstva i brodogradnje, Zagreb.

[4] Јаневски, Д. (2018): *Развојни електронски плочи со микроконтролери*, Дипломска работа, Воена академија „Генерал Михаило Апостолски“, Скопје.

[5] Kaur, G.,. Bhatia, N. (2019): Quickstego – an image steganography gear, *International Journal of Scientific Research in Computer Science. Applications and Management Studies*, ISSN 2319 – 1953.

[6] Маркудова, Љ., Јовановска, И., Домазетовска, J. (2010): *Дигитална електроника и микропроцесори*, Учебник за III година. Скопје.

[7] Сервини. J., Сервини, Ж. (2011): *Дигитална електроника и микропоцесори.* II (втора) година електротехничка струка електротехничар за електроника и телекомуникации, Министерство за образование и наука на Република Северна Македонија.

[8] Blum, J. (2020): *Exploring Arduino: Tools and Techniques for Engineering Wizardry*, John Wiley & Sons, Inc., Canada, ISBN: 978-1-119-40537-5.

[9] Hobring, L., Söderberg P. (2014): *A Sensor Network for the Internet of Things: Integrated with a Bidirectional Backend*, Blekinge Institute of Technology, Sweden.

[10] Margolis, M., Jepson, B., Weldin, N. R. (2020): *Arduino Cookbook: Recipes to Begin, Expand, and Enhance Your Projects*, O`Rielly Media Inc., United States of America, ISBN-978-1-491-90352-0.

[11] Thompson, M. (2018), *Arduino: The essential step by step guide to begin your own amazing projects*, CreateSpace Independent Publishing Platform, ISBN-9781721076628.

[12] Cameron, N. (2019): *Arduino Applied: Comprehensive Projects for Everyday Electronics*, Springer Science + Business Media Finance Inc (SSBM Finance Inc), Edinburgh, UK, ISBN-13 (electronic): 978-1-4842-3960-5.

[13] Cliff, O. (2014): *Then and now: A brief history of single board computers*, Electronic Design Uncovered – Issue 06, Newark, United States of America (USA).

[14] Ristić, S. (2010): *Elektronske komponente*, Predavanja, Godina: I. Semestar: II. Elektronski fakultet Niš, Republika Serbija.

[15] Мустафовски, Р. (2022): *Примена на компјутери со една плоча за изградба на радарски систем за детекција на објекти на кратки растојанија,* Магистерски труд, Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за електротехника и информациски технологии, Скопје.

[16] Eckert, S. M. (2019): *Arduino Uno Progamming: Programmable circuit boards and coding programms of your choice to run on your computer*, Kindle edition, ISBN-B086Y4F5QD.

[17] Osborne, W. P. (2017): *Learning to Program in Arduino™ C*: 18 lessons, from setup() to robots, CreateSpace Inc., United States of America. ISBN-978-0-9981287-1-9.

[18] *Then and now: a brief history of single board computers* [Accessed on 10.01.2024] https://www.electronicspecifier.com/products/communications/then-and-now-a-briefhistory-of-single-board-computers

[19] *Arduino Radar Project* [Accessed on 10.01.2024] https://howtomechatronics.com/projects/arduino-radar-project/

[20] *Arduino Radar Project* – Version 2.0 [Accessed on 10. 1. 2024], https://create.arduino.cc/projecthub/MakerRobotics/arduino-radar-version-2-0-24371e?ref=tag& ref_id=radar&offset=2

Journal of Electrical Engineering and Information Technologies, Vol. **9,** No.1, pp. 71–74 (2024)
In print: ISSN 2545–4250
On line: ISSN 2545–4269

INSTRUCTIONS FOR AUTHORS

The *Journal of Electrical Engeneering and Information Technologies* is published twice yearly. The journal publishes **original scientific papers, short communications, reviews** and **professional papers** from all fields of electrical engineering.

The journal also publishes (continuously or occasionally) the bibliographies of the members of the Faculty, book reviews, reports on meetings, informations of future meetings, important events and data, and various rubrics which contribute to the development of the corresponding scientific field.

Original scientific papers should contain hitherto unpublished results of completed original scientific research. The number of pages (including tables and figures) should not exceed 15 (28 000 characters).

Short communications should also contain completed but briefly presented results of original scientific research. The number of pages should not exceed 5 (10 000 characters) including tables and figures.

Reviews are submitted at the invitation of the Editorial Board. They should be surveys of the investigations and knowledge of several authors in a given research area. The competency of the authors should be assured by their own published results.

Professional papers report on useful practical results that are not original but help the results of the original scientific research to be adopted into scientific and production use. The number of pages (including tables and figures) should not exceed 10 (18 000 characters).

Acceptance for publication in the Journal obliges the authors not to publish the same results elsewhere.

SUBMISSION

The article and annexes should be written on A4 paper with margins of 2.5 cm on each side with a standard font Times New Roman 11 points and should be named with the surname of the first author and then if more and numbered. It is strongly recommended that on MS Word 2003 or MS Word 2007 and on PDF files of the manuscript be sent by e-mail:

JEEIT@feit.ukim.edu.mk.

A letter must accompany all submissions, clearly indicating the following: title, author(s), corresponding author's name, address and e-mail addres(es), suggested category of the manuscript and a suggestion of five referees (their names, e-mail and affiliation).

Articles received by the Editorial Board are sent to two referees (one in the case of professional papers). The suggestions of the referees and Editorial Board are sent to the author(s) for further action. The corrected text should be returned to the Editorial Board as soon as possible but in not more than 30 days.

PREPARATION OF MANUSCRIPT

The papers should be written in the shortest possible way and without unnecessary repetition.

The original scientific papers, short communications and reviews should be written in English, while the professional papers may also be submitted in Macedonian.

Only SI (Système Internationale d'Unites) quantities and units are to be used.

Double subscripts and superscripts should be avoided whenever possible. Thus it is better to write $\nu_3(PO_4)$ than $\nu_{3_{PO_4}}$ or exp(–E/RT) than $e^{-E/RT}$. Strokes (/) should not be used instead of parentheses.

When a large number of compound have been analyzed, the results should be given in tabular form.

Manuscript should containt: title, author(s) full-name(s), surname(s), address(es) and e-mail of the corresponding author, short abstract, key words, introduction, experimental or theoretical back-ground, results and discussion, acknowledgment (if desired) and references.

The **title** should correspond to the contents of the manuscript. It should be brief and informative and include the majority of the key words.

Each paper should contain an **abstract** that should not exceed 150 words and **3–5 key words**. The abstract should include the purpose of the research, the most important results and conclusions.

The **title**, **abstract** and **key words** should be translated in Macedonian language. The ones written by foreign authors will be translate by the Editorial Board.

In the **introduction** only the most important previous results related to the problem in hand should be briefly reviewed and the aim and importance of the research should be stated.

The **experimental** section should be written as a separate section and should contain a description of the materials used and methods employed – in form which makes the results reproducible, but without detailed description of already known methods.

Manuscripts that are related to **theoretical studies**, instead of experimental material, should contain a sub-heading and the **theoretical background** where the necessary details for verifying the results obtained should be stated.

The **results** and **discussion** should be given in the same section. The discussion should contain an analysis of the results and the **conclusions** that can be drawn.

Figures (photographs, diagrams and sketches) and **mathematical formulae** should be inserted in the correct place in the manuscript, being horizontally reduced to 8 or 16 cm. The size of the symbols for the physical quantities and units as well as the size of the numbers and letters used in the reduced figures should be comparable with the size of the letters in the main text of the paper. Diagrams and structural formulae should be drawn in such a way (e.g. black Indian ink on white or tracing paper) as to permit high quality reproduction. The use of photographs should be avoided. The tables and the figures should be numbered in Arabic numerals (e.g. Table 1, Figure 1). Tables and figures should be self-contained, i.e. should have captions making them legible without resort to the main text. The presentation of the same results in the form of tables and figures (diagrams) is not permitted.

Figures and tables must be centred in the column. Large figures and tables may span across both columns (Figure 1).

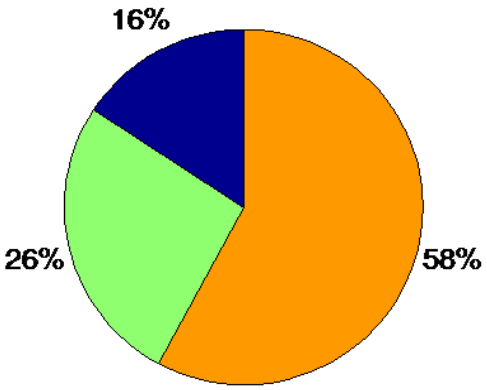


Fig. 1. Example of a graph and a single-line caption (collour)

Graphics may be full colour. Please use only colours which contrast well both on screen and on a black-and-white hardcopy because the Journal is published in black-and-white, as shown in Figure 2. The colour version is only for the electronic version of the Journal.

Please check all figures in your paper both on screen and on a black-and-white hardcopy. When you check your paper on a black-and-white hardcopy, please ensure that:

– the colours used in each figure contrast well,

– the image used in each figure is clear,

– all text labels in each figure are legible.

Please check all figures in your paper both on screen and on a black-and-white hardcopy. When you check your paper on a black-and-white hardcopy, please ensure that the image used in each figure is clear and all text labels in each figure are legible.

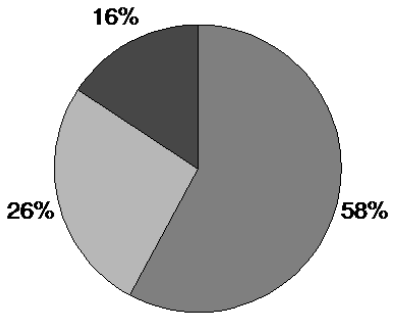


Fig. 2. Example of a graph and a single-line caption (black-and-white)

Fig. 3. Example of an image as it will appear at the electronic version of the Journal and a multi-line caption

Footnotes are also not permitted.

The **reference** should be given in a separate section in the order in which they appear in the text. The surname of one or two authors may be given in the text, whereas in the case of more than two authors they should be quoted as, for example:

Examples of reference items of different categories shown in the References section include:

- example of a book in [1]
- example of a book in a series in [2]
- example of a journal article in [3]
- example of a conference paper in [4]
- example of a patent in [5]
- example of a website in [6]
- example of a web page in [7]
- example of a databook as a manual in [8]
- example of a datasheet in [9]
- example of a master/Ph.D. thesis in [10]
- example of a technical report in [11]
- example of a standard in [12]

All reference items must be in 9 pt font. Please use Regular and Italic styles to distinguish different fields as shown in the References section. Number the reference items consecutively in square brackets (e.g. [1]).

When referring to a reference item, please simply use the reference number, as in [2]. Do not use "Ref. [3]" or "Reference [3]" except at the beginning of a sentence, e.g. "Reference [3] shows …". Multiple references are each numbered with separate brackets (e.g. [2, 3], [4–8]).

The **category** of the paper is proposed by the author(s), but the Editorial Board reserves for itself the right, on the basis of the referees' opinion, to make the final choice.

Proofs are sent to the author(s) to correct printers' errors. Except for this, alterations to the text are not permitted. The proofs should be returned to the Editorial Board in 2 days.

The author(s) will receive, free of charge, 1 reprint of every paper published in the Journal.

REFERENCES

[1] Surname, N(ame).; Surname, N(ame). (Year): *Name of the Book*, Publisher.

[2] Surname, N(ame).: Surname, N(ame). (Year): *Name of the Book*, Name of the Series. Publisher, **vol.** XXX.

[3] Surname, N(ame).; Surname N(ame). (Year): Title of the article, *Name of the Journal*, **Vol. XX,** No. XX, pp. XXX–XXX.

[4] Surname, N(ame).; Surname N(ame). (Year): Title of the article, *Proceedings of the Conference (Name)*, **Vol. XX,** pp. XXX–XXX.

[5] Surname, N(ame).; Surname N(ame). (Date dd. mm. yyyy): *Name of the Patent*, Institution that issued the patent & Number of the patent.

[6] N.N. (Year): *The XXX web site*, web address.

[7] Surname, N. (Year): *XXX homepage on XXX*, web address.

[8] N.N. (Year): *Title of the Manual*, Name of the Organization.

[9] N.N.: *XXX data sheet*, Name of the Organization.

[10] Surname, N. (Year): *Title of the Thesis*, Master/Ph.D. thesis (in Language), Institution.

[11] Surname, N(ame)., Surname, N(ame). (Year): *Title of the Report*, organization that issued the report, Number of the report.

[12] Institution that issued the standard, *Name of the Standard*, & Number of the standard (Year).