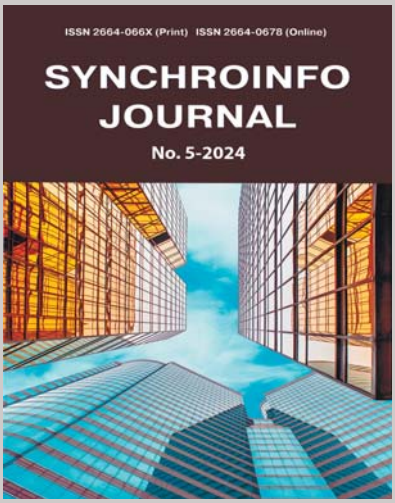
CONTENT

Vol. 10. No. 5-2024



Published bi-monthly since 2015

ISSN 2664-0678 (Online)
ISSN 2664-066X (Print)

Publisher
Institute of Radio and Information Systems (IRIS), Vienna, Austria

Address:
1010 Wien, Austria, Ebendorferstrasse 10/6b
media-publisher.eu/synchroinfo-journal

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

ANALYSIS OF THE ELEMENT BASE FOR OPTICAL TRANSMISSION SYSTEMS AND RESEARCH OF SYNCHRONIZATION SYSTEMS COMPONENTS CHARACTERISTICS

Alexander L. Makarevich [1], **Yaroslav O. Lipadat** [1], **Sergey M. Sokovnich** [1],

Yulia V. Zakharova [1], **Anton A. Taban** [2]

[1] State Educational Institution "PSU named after T.G. Shevchenko", Tiraspol, Moldova, Transnistria;

mccar-bendery@mail.ru, jaroslavlipadat@gmail.com, s_sokovnich@rambler.ru, zakharova.yulia@bk.ru

[2] MIET, Moscow, Zelenograd, Russia;

b9rs9rk@gmail.com

ABSTRACT

The article presents an analysis of the literature and discusses examples of developments of some photonic integrated circuits (PICs) used as switches that control the formation of flows in optical packet-switching networks. The trends discussed are also applicable to other classes of circuits and network devices, in particular modules of more complex systems. The article presents the results of studies of the characteristics of synchronization system components based on phase-locked loop (PLL) devices capable of providing synchronous operation of various systems using orthogonal frequency division multiplexing (OFDM) and multiple input/output (MIMO) technologies. The results show the possibility of using these components in devices designed to operate in optical information transmission systems and will allow creating the necessary frequency synthesizer's blocks for constructing and implementing them in the form of specialized ASICs manufactured using CMOS technology.

KEYWORDS: *silicon photonics, integrated optics, III-V semiconductor materials, PLL devices, frequency synthesizers, voltage-controlled oscillators (VCO), phase detectors (PD)*

DOI: 10.36724/2664-066X-2024-10-5-2-15

Received: 20.08.2024
Accepted: 22.09.2024

Citation: A.L. Makarevich, Ya.O. Lipadat, S.M. Sokovnich, Yu.V. Zakharova, A.A. Taban, "Analysis of the element base for optical transmission systems and research of synchronization systems components characteristics" *Synchroinfo Journal* **2024**, vol. 10, no. 5, pp. 2-15.

Licensee IRIS, Vienna, Austria.

Introduction

Switches that control the formation of flows in optical packet switching networks currently require the most careful attention from specialists in the field of infocommunication technologies. In our opinion, these devices are in demand both by the market and by the ongoing progress in the development of telecommunications and communication systems.

Silicon photonics (SiPh) is a revolutionary technology in the field of integrated photonics, which has developed rapidly over the past two decades. Various high-performance Si and Ge/Si-based components have been developed on this platform, which enable the creation of complex photonic integrated circuits (PICs) with a small footprint [1]. The limited capabilities of electronic devices in modern data transmission networks are the main obstacle to the development of high-speed data transmission networks. The emergence of optical systems with terabit and petabit data rates [2], implemented on the basis of WDM wave multiplexing technologies, places the highest demands on control electronics responsible for the formation of frame formats that not only correspond to the Optical Transport Hierarchy (OTH), but also the implementation of SDM networks using spatial multiplexing (SDM technology) for high-bandwidth information transmission [3].

The use of OFDM and MIMO technologies in optical networks and radio channels for high-speed data transmission also places increased demands on synchronization systems and noise-resistant coding methods [4, 5, 6]. High-quality synchronization plays a special role in digital radio communication and radio navigation systems [7, 8].

Analysis of developments for the creation of optical network switches

Frequency synthesizers

The main means of maintaining synchronous operation of high-speed data transmission networks are phase-locked loop (PLL) devices, the creation of which requires: phase detectors (phase comparators), voltage-controlled generators (VCO), frequency synthesizers (FS), which themselves have the widest application [9]. In particular, FS in one form or another are present in virtually all electronic systems, such as:

- c ntrol and measuring equipment,
- r ceiving and transmitting equipment,
- v rious communication systems (including new projects such as WLAN, 5G, etc.),
- radar equipment,
- medical equipment [9].

The emergence and widespread use of the microwave midrange became possible with the industrial development of the production of specialized microcircuits (ASIC) manufactured using CMOS technology with submicron design standards.

Our previous studies of the characteristics of PLL components [10, 11, 12] showed the possibility of operation of these devices at frequencies up to 7 GHz, which is quite acceptable for use in switches intended for use in optical data transmission systems. But this was obtained on models of CMOS transistors with design standards of 65 and 90 nm. Naturally, with a decrease in design standards, the operating frequencies will increase. In the work of Professor E. Sicard [13] from Microwind, the results of modeling a ring generator on three inverters manufactured using CMOS technology with design standards of 7 nm are presented, which show the possibility of generators operating at frequencies from 50 to 100 GHz.

Such generators are necessary when creating the microwave MF range. The principles of constructing frequency synthesizers for a wide variety of applications, including optical data transmission systems, are described both in the classic work of V. Manassevich [14] and in the works of other authors [9, 15, 16]. At the same time, we believe that the use of complex functional blocks in specialized microcircuits manufactured using CMOS technology with submicron design standards will allow us to successfully solve the problems of creating devices for high-speed optical data transmission networks [17, 18, 19].

As a conclusion after analyzing the literature, we can say that the components of the PLL device are the most effective solution for creating microwave frequency synthesizers.

Multiplexers/Demultiplexers

Formation of the transmitted information flows in the information transmission networks is traditionally provided by devices previously called compression equipment, but with the transition to digital technology, this compression/decompression function began to be performed by multiplexers/demultiplexers (MUX/DMX). To implement MUX/DMX, decoders are needed, which determine which channels and in what order will be transmitted during transmission and then distributed to users on the receiving side. Moreover, network devices of the MUX/DMX type must operate synchronously and, if possible, in-phase. This is exactly what can be provided by functional blocks implemented as part of specialized VLSI, manufactured using CMOS technology with submicron design standards [20].

The implementation of conventional digital synchronously operating multiplexers and demultiplexers does not cause any difficulties when modeling their operation even for students. But in the case of using OFDM technology, i.e. frequency multiplexing in the optical wavelength range, it will require first choosing the most optimal algorithm, and most importantly, choosing a noise-immune coding method to overcome the problems of interchannel interference. To do this, it is necessary to use the capabilities of MatLAB, which has the ability to select algorithms and methods of noise-immune coding. And only then, after choosing the algorithms and coding methods, it will be necessary to move from the register transfer level (RTL) of processing the transmitted information to circuit modeling and topological implementation of functional blocks in microcircuit crystals using a set of photomasks.

Multiplexers/demultiplexers are key components for constructing channels using MDM (Mode Division Multiplexing) technology, which provides unprecedented bandwidth scaling that can eliminate communication bottlenecks in high-density on-chip interconnects since each mode of one wavelength becomes a separate data transmission channel [20].

Mode multiplexers combine adiabatic couplers with subwavelength gratings (SWG). Figure 1 shows the schematic of the proposed SWG-based multiplexer [20].

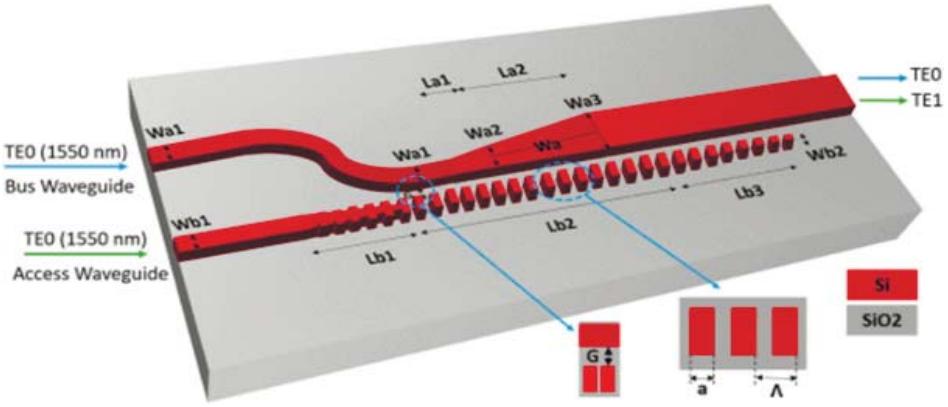


Figure 1. Schematic diagram of the proposed dual-mode multiplexer

The same work presents the results of the performance evaluation of the proposed device. The experimental setup diagram is shown in Figure 2.

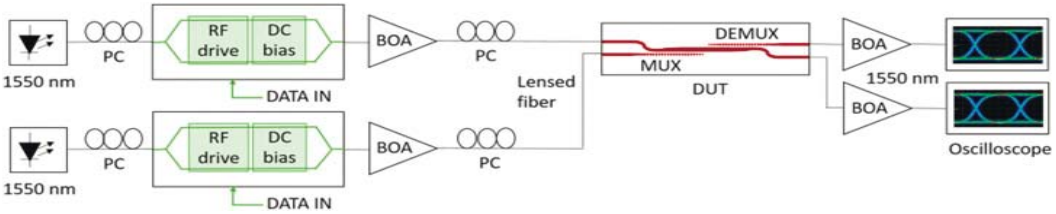


Figure 2. Experimental setup for on-chip dual-mode demultiplexing

Figures 3(a) and (b) show the input and pre-amplified optical signal modulated at 40 and 64 Gbps, respectively. The output signal was then amplified using a polarization-insensitive semiconductor optical amplifier (Thorlabs S7FC1013S). The optical signals corresponding to the input/output pairs I1/O1 and I2/O2 were then amplified and acquired using a Keysight Infinium DCA-X 86100D wideband oscilloscope. Figures 3(c-f) show open and clear eye diagrams for each of the demultiplexed signals, indicating the high performance of the device and low crosstalk.

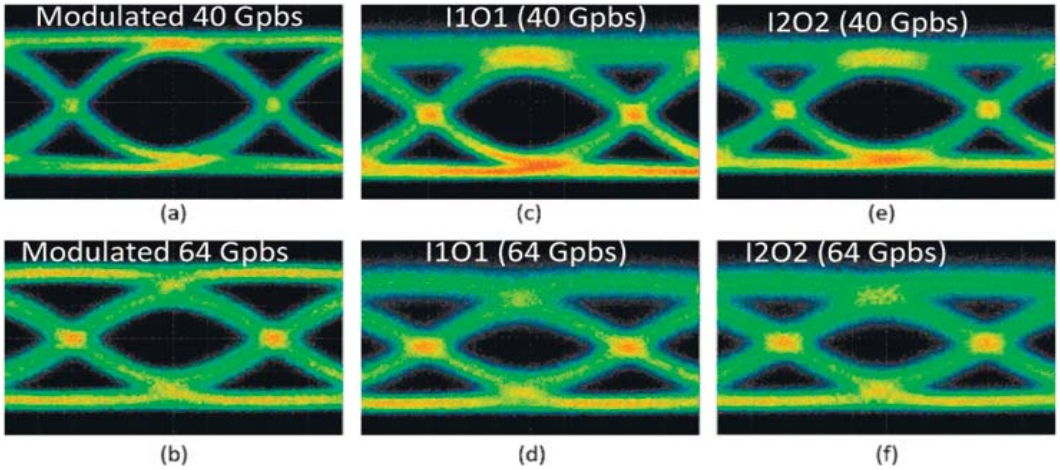


Figure 3. Eye diagrams of the modulated input signal with rates of (a) 40 Gbit/s and (b) 64 Gbit/s. Eye diagrams of the demultiplexed signal with insertion loss I1/O1 with rates of 40 Gbit/s (c and e) and 64 Gbit/s (d and f)

The device proposed by the authors of [20] has a very compact size with a coupling area of 8.5 μm, while the length of the entire MDM channel (multiplexer and demultiplexer) is only 55 μm. The device was fabricated on a standard SOI platform using electron beam lithography technology, and butt jointing was used to experimentally verify its performance. The MDM channel demonstrated measured IL and CT values at 1550 nm wavelength better than 0.9 dB and –18.7 dB, respectively. Covering a wavelength range of 200 nm, it achieved a maximum interference and crosstalk level of 2.3 dB and –18.6 dB, respectively. The system was demonstrated using NRZ modulated signals at 40 Gbps and 64 Gbps. Open and clear eye diagrams were obtained, confirming the feasibility of using the device for on-chip demultiplexing.

As a conclusion after analyzing the literature, it can be said that multiplexers and demultiplexers are the basis for creating switches that control the flow of transmitted information in optical systems, while the synchronicity of their operation will be ensured by PLL devices implemented as part of specialized microcircuits manufactured using CMOS technology with submicron design standards.

Switches for managing information transmission in optical networks

Over the past few decades, network traffic has been growing at an exponential rate and has been efficiently accommodated using WDM and more efficient coding schemes that require coherent synchronization [3]. There is no sign that the trend of increasing network traffic will stop anytime soon, and we are approaching the day when the capacity of ubiquitous single-mode fiber will be fully utilized.

It seemed that with the transition from decade-step and coordinate automatic telephone exchanges to electronic switching systems, spatial switching would finally be replaced by temporal switching. However, spatial domain multiplexing (SDM) for high-capacity data transmission is a promising solution with scalability potential to meet future bandwidth needs. At the same time, there is still a large technological gap between current designs of WDM optical communication systems and the implementation of SDM networks. In our opinion, the work of Dan M. Marom, Miri Blau [3] lays the foundations for the design of switching nodes for future WDM-SDM optical networks.

We present some excerpts from this work, illustrating the principles of constructing switches for such optical networks.

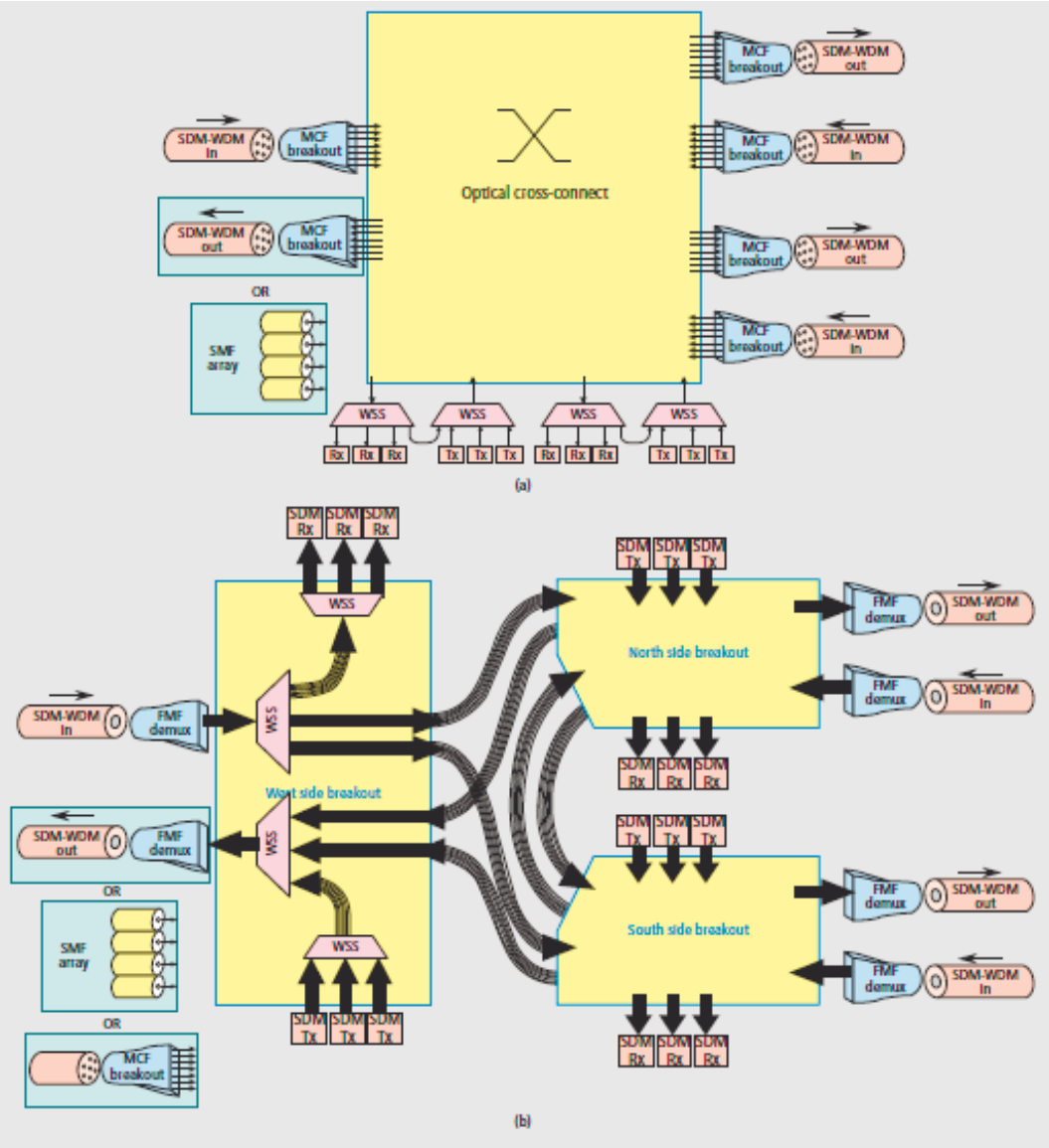


Figure 4. Switching node diagrams for implementation:
a) spat l routing of the entire communication band in accordance with the spatial regime; b) wave routing of all nodes according to wavelength

Here, the formation of streams for transmitting information is intended for packet switching networks, i.e. for IP networks.

SDM transmission is a promising solution to the SMF capacity constraint, but addressing the physical elements of SDM of new fiber types supporting optical amplifiers and mode multiplexers without careful attention to the capabilities of the optical networks misses an important element of the overall proposal. This paper [3] highlights some of the implications of the design of a WDM-SDM optical mesh network, with particular attention to the design of the switching nodes through which information flows must be provided. It identifies four categories of capacity granularity that must be prepared and applied in the spatial and wavelength domains. Each category can be implemented using different optical switching devices at the network nodes, which affects the complexity and cost of implementation, as well as flexibility and scalability.

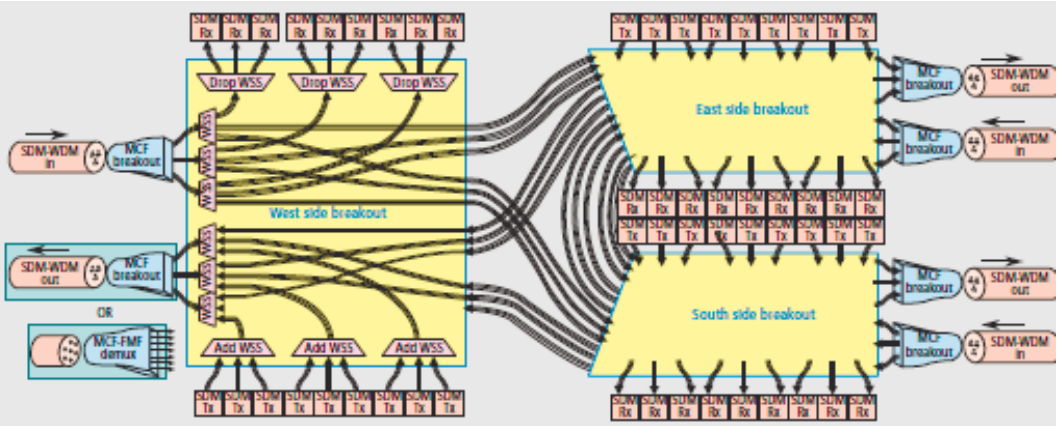


Figure 5. Schematic diagram of a switching node for implementing hybrid granularity of partial-space and full-wavelength switching, routing of spatial superchannels covering WS spatial subgroups

At this early stage, it is premature to conclude whether there is an optimal solution for a WDM-SDM optical network. This needs to be assessed for specific network designs and traffic [3]. Different network applications are likely to have different solutions. The evaluation of the overall optical network needs to take into account the physical layer attributes, the expected scale of information flows and churn, how efficiently they can be implemented given the minimum granularity of the bandwidth routed by the network, the probability of blocking due to contention for the provision of information flows, and the cost of implementation, among other things.

The WDM-SDM mesh node switching solutions that are the focus of this paper and a key factor in network performance and cost can be assessed using a routing power metric borrowed from reconfigurable wavelength add/drop node designs [21, 22].

The routing capacity metric can be used as a measure of the number of states and connections for a switching node and will decrease with greater switching granularity, but this loss of flexibility is favorably offset by lower implementation costs.

Thus, a complete analysis requires the participation of various groups of experts and will likely require a concerted effort from many researchers in this field to analyze the performance levels and benefits offered by WDM-SDM optical networks.

Integrated circuits for optical networks

Photonic integrated circuits (PICs) enable the miniaturization of optical data transmission systems by integrating key optical functions on a single chip. SiPh is emerging as an important platform for implementing such PICs, as existing CMOS technology can be used to implement these circuits on 200 nm and 300 nm diameter wafers with high yield. In addition, the high refractive index enables the creation of compact optical circuits and high-speed detectors and modulators due to the strong light-matter interaction. In addition to using Si waveguides, silicon nitride (Si3N4) waveguides can also be implemented, providing lower losses and a wider range of operating wavelengths. These Si3N4 waveguides can either be combined with Si waveguides on a single platform or be a separate passive platform [23].

The concept of micro-transfer technology (μTP) is to pre-fabricate components from A3B5 materials on a base plate. This is illustrated in Figure 6(a). A special feature of the μTP approach is that the spacer layer must be integrated with the other device layers. After patterning the devices in dense matrices on the base plate, the components are bonded to either the layer or the dielectric substrate, after which the interlayer dielectric is selectively etched away, making the patterned components free-standing and positioned near the connection lines.

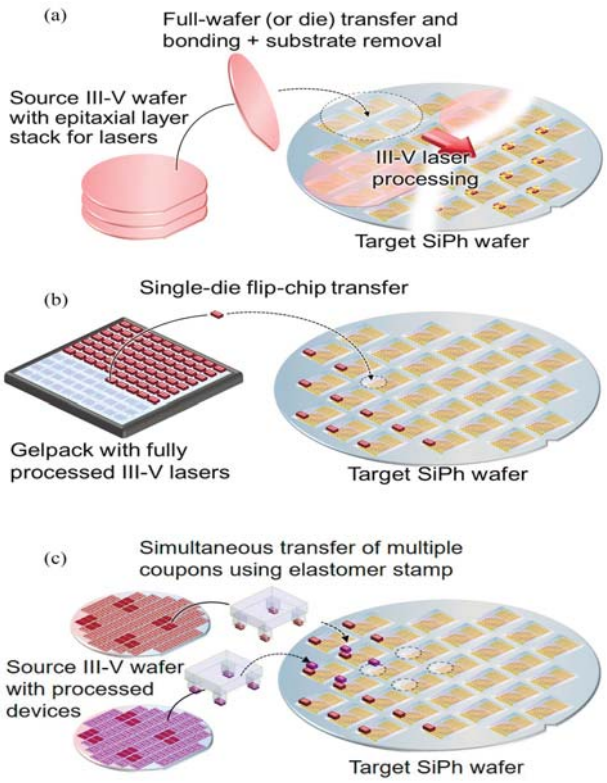


Figure 6. Illustration of the integration of A3B5 materials on Si on a SiPh chip wafer via: (a) wafer-to-wafer bonding; (b) flip-chip; and (c) microtransfer printing

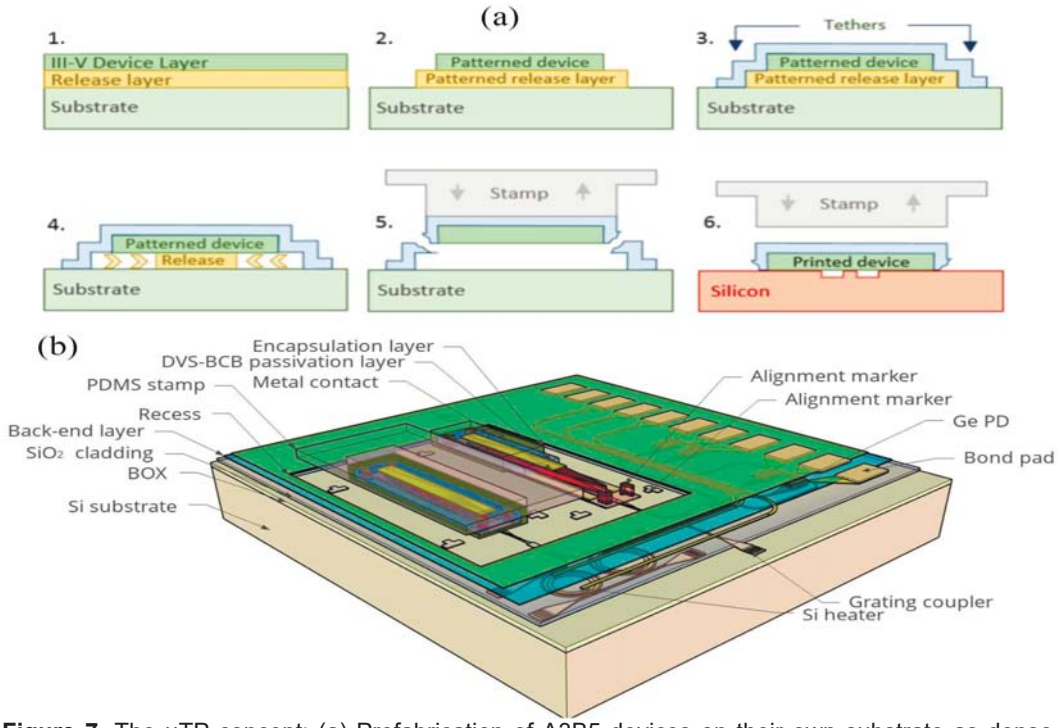


Figure 7. The µTP concept: (a) Prefabrication of A3B5 devices on their own substrate as dense matrices and subsequent integration of µTP onto the target Si substrate; (b) Illustration of the integration of A3B5 devices onto a Si base wafer (on-Si) aligned with the inner layers. This requires only local etching of the contact windows to ensure tight metallic contact between the A3B5 components and the layers on the Si substrate

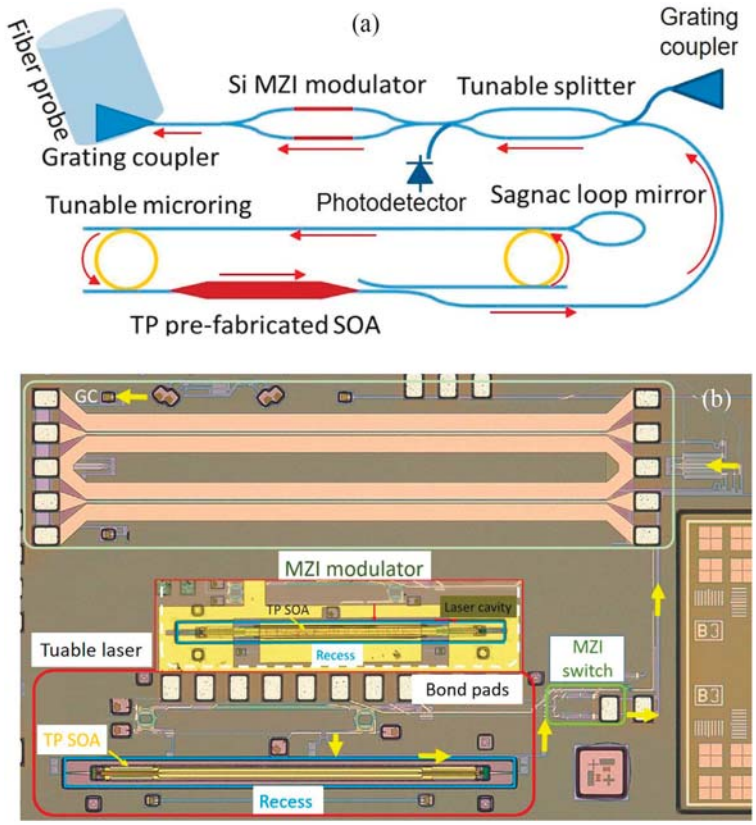


Figure 8. Schematic diagram of the embedded optical transmitter (a). At the bottom is a microscopic image of a photonic integrated circuit (PIC) with a III-V amplifier printed by microtransfer in a pre-etched cavity. The inset microscopic image shows the SOA microtransfer amplifier after metallization

The first fabricated tunable III-V laser on silicon was tested at 20°C without a modulator. The differential resistance of the μTP of the III-V SOA amplifier was 6.5 Ω at 130 mA, and the maximum waveguide-coupled power was 2 MW at 130 mA bias current.

The laser response threshold was about 100 mA at 1553 nm, and the maximum power conversion efficiency was about 0.7%. By simultaneously turning on both the Vernier-assisted micro-ring resonator heaters in the phase section, a tuning range of more than 40 nm was achieved, which is also shown in Figure 8(a). Second, optical backtransmission experiments were performed in a high-speed setup at 20°C.

An arbitrary waveform generator (AWG) was used to generate two identical PRBS signals of length 2^9-1 in return-to-zero code. These signals were amplified by RF amplifiers, combined with the correct bias levels by a pair of bias tees, and then injected into the MZI modulator by a GSG RF sensor.

The bias current supplied to the on-chip SOA was maintained at 130 mA. The modulated optical signal was detected by a commercial high-speed optical receiver after being amplified by an EDFA. A measuring instrument was used to represent the output electrical signal from the optical receiver. The opening of the eye diagrams was detected at 28 and 40 Gbps in the C-band wavelength. The results are shown in Figure 9(b).

The devices described in [23] are promising proofs of concepts that highlight the potential of μTP technology for creating heterogeneous PICs. Since the technology is very versatile, other demonstrations are currently underway focusing on μTP lasers on InAs/GaAs quantum dots, Ce:YIG magneto-optical materials for optical isolators, LiNbO3 with periodic polarization for nonlinear optics, BiCMOS electronics, etc. However, the use of this technology as a mass production technology is still a long way off.

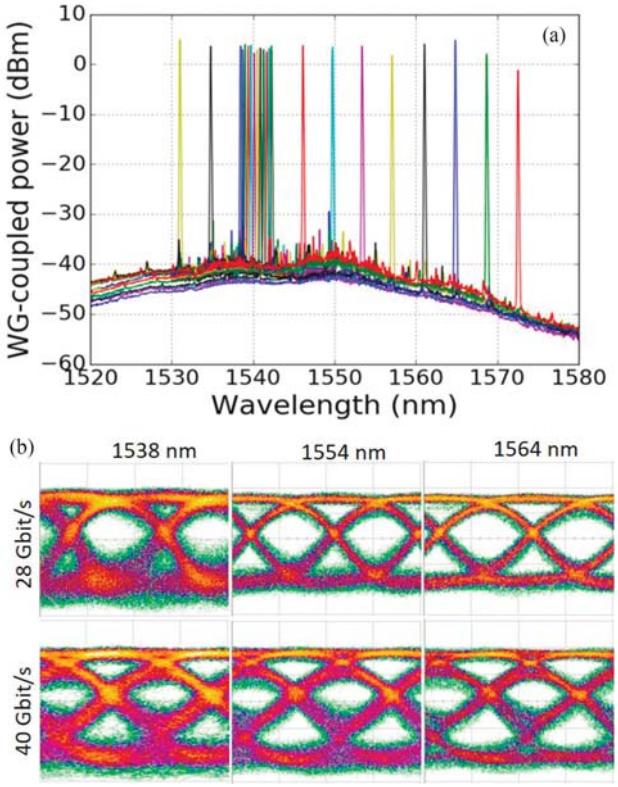


Figure 9. Tuning wavelengths greater than 40 nm in C-band (a). Measured eye diagrams of NRZ code with data rates of 28 Gbit/s and 40 Gbit/s for different wavelengths (b)

Work is underway to develop this technology for 200mm and 300mm wafers. It is necessary to continuously improve the performance of the devices, and also to study the possibilities of increasing their performance and reliability. If the problems associated with these issues can be overcome, we believe that μTP technology has a good future for the creation of next-generation photonic/electronic integrated circuits.

Research of characteristics of components of synchronization systems

Here we will consider the results of our research obtained as a result of circuit simulation of the operation of PLL devices and their components intended for manufacturing using CMOS technology as part of specialized ASIC microcircuits operating in equipment for a wide variety of applications [10, 11, 12, 24, 25].

In one of our previous works [26], related to the study of synchronization in on-board systems, we simulated the operation of PLL device components implemented on CMOS transistors with design standards of 90 and 65 nm.

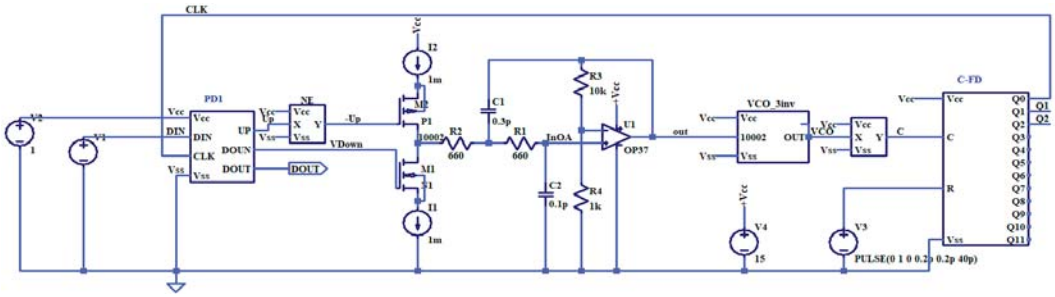


Figure 10. PLL circuit implemented on 90 nm CMOS transistors containing a phase detector (PD), an op-amp active filter, a voltage-controlled oscillator (VCO) and a counter-frequency divider (C-FD)

The main modeling tool was the LTSpice program, the type of transistor models used was level = 3, and most of the model parameter values for the specified design standards were borrowed from the sitehttps://microwind.net/and supplemented by us with the values of resistance and capacitance of the source and drain regions of the MOS transistors.

In this work, we focused on the performance studies of several variants of VCO generator design that can be the basis for designing frequency synthesizers required for use in OFDM technology. According to recent publications [28, 29], special attention is paid to low-jitter digital PLLs that provide synchronous operation in high-speed data transmission systems, including optical transmission systems.

In this study, we would like to evaluate the possibility of using a PLL device with the obtained parameters in switching and control systems for high-performance quantum networks [1-4]. It is these networks and systems that place increased demands on the synchronous operation of numerous transmitters and receivers required for their implementation. Moreover, the switching speeds in such networks should be significantly higher than those used in conventional networks. We are talking about working according to the Precision Time Protocol (PTP) and the possibility of achieving subnanosecond synchronization, but the accuracy of synchronization in real networks will still be limited for objective reasons [15]. The switching process in the spatial domain (SDM – Spice Domain Multiplexing) itself will require new algorithms, since this technology is associated with software-defined networks (Soft-Ware Defined Networks – SDN) [1, 4]. Information in them is usually presented in packet form (IP) and can contain frames of any hierarchy: PDH, SDH, OTH or Ethernet and even transport networks using MPLS technology. To control and monitor the correct transmission of such frames, specialized devices are required that have high-quality synchronization systems that use high-speed PLL components and are also compatible with monitoring the correctness of the transmitted information.

Since OFDM and MIMO technologies have been used for high-speed data transmission in both radio channels and optical networks [4], the first task we will try to solve using LTSpice is to determine the frequency range generated by C-FD, which will then allow us to estimate the frequency locking times. Considering the division factor of a 12-bit counter, which is 4096, with a maximum frequency at the Q0 output of about 3.5 GHz, the frequency at the Q11 output will be about 0.85 MHz.

Therefore, additional studies were conducted to determine the frequency spectrum generated by the internal VCO generator. Figure 2 shows the oscillograms of the input V(din), internal V($g_d1), V(vco), V(c) and the output signals of the least significant bits Q0 – Q2 from the PLL device counter.

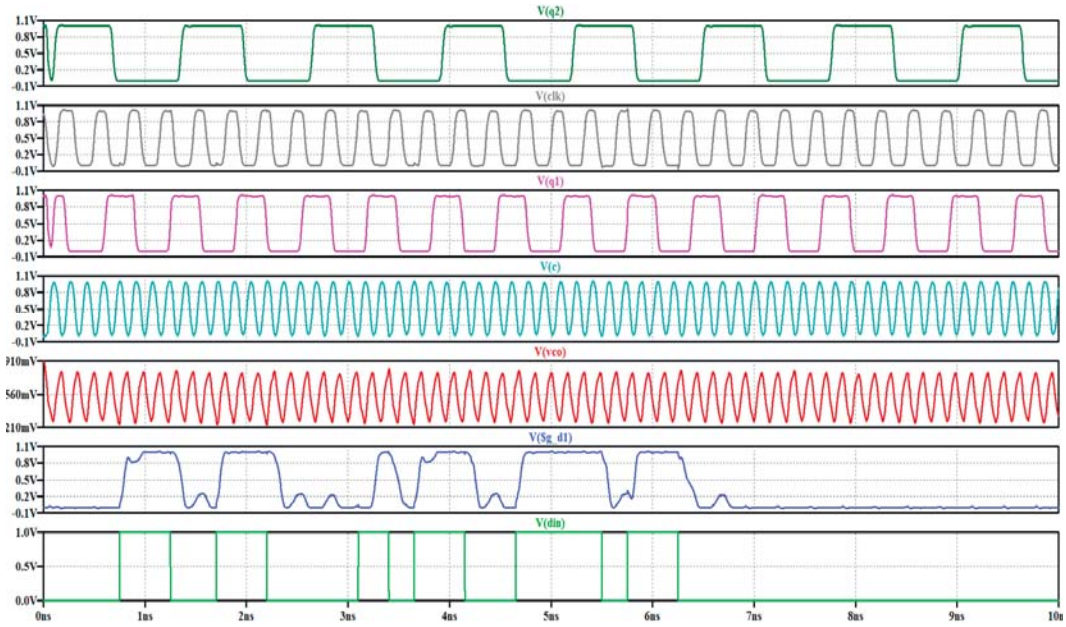
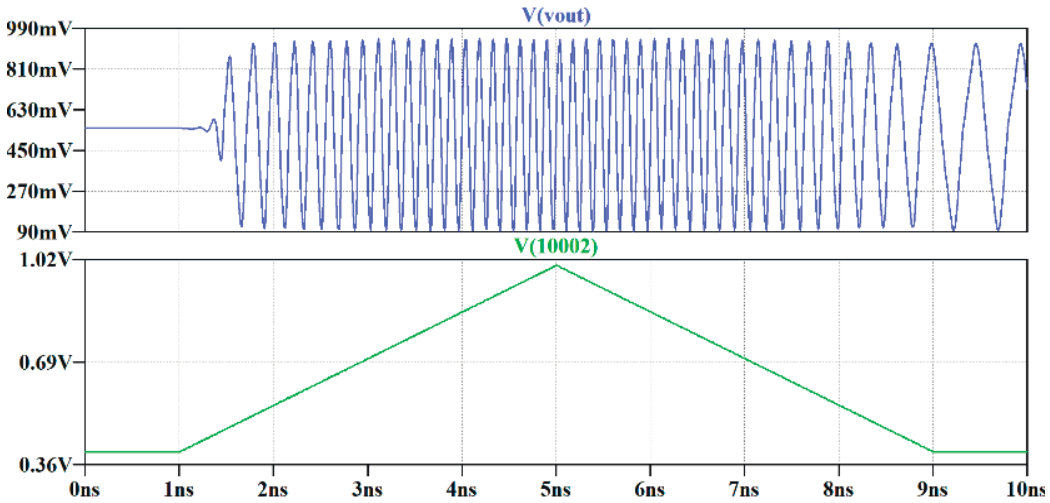


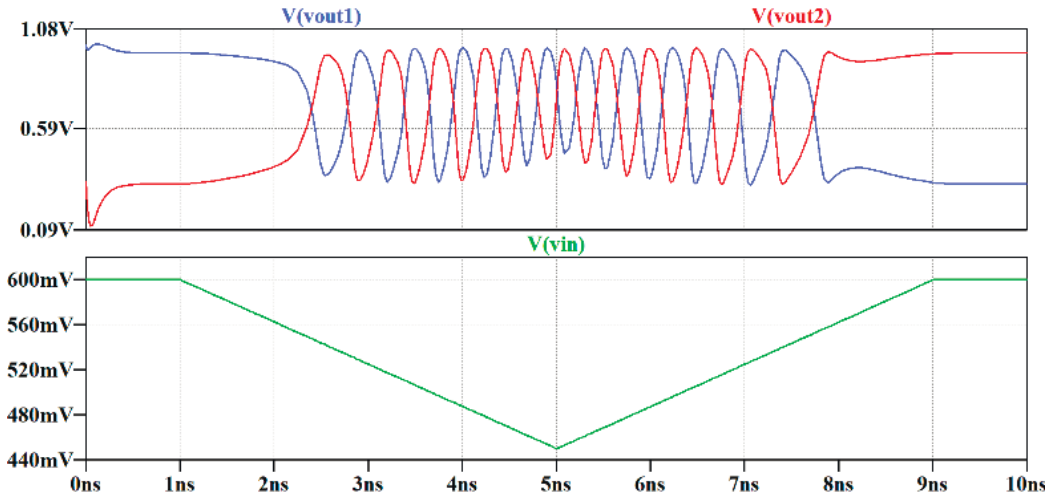
Figure 11. PLL signal oscillograms

Internal signals confirm the correct operation of the phase detector and the UP and DOWN signal extractor. The amplitude of the V(vco) signal is less than required, and for this purpose the INV5 inverter is used to increase the amplitude of the V(c) signal. As a result, the signals at the outputs of the least significant digits of the Q0(Vclk), Q1, and Q2 counters have the required level and correspond to the operating algorithm of the summing binary counter.

To evaluate the performance of the voltage-controlled generator VCO, an experiment was conducted, the results of which are shown in Figures 12a and 12b.



a)



b)

Figure 12. Oscillograms of VCO output signals on inverters (a) and multivibrator (b) when changing the control voltage

The VCO generator we use is built on a ring of three inverters controlled by a current mirror and its diagram is shown in Figure 13.

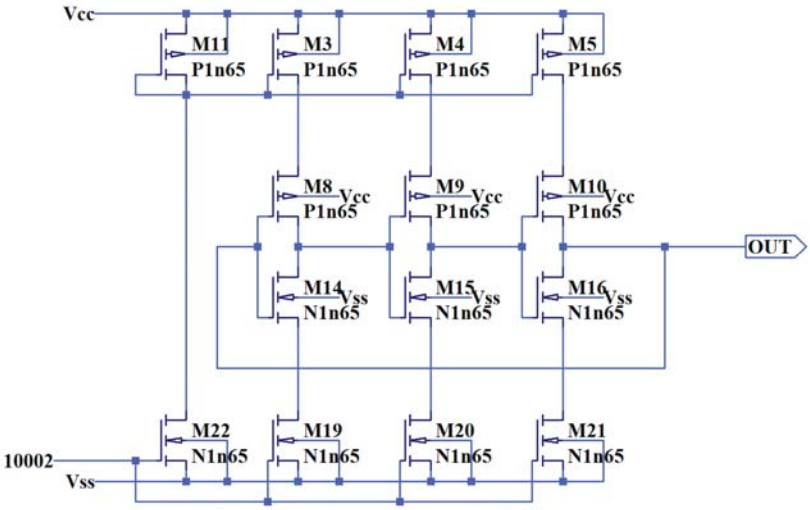


Figure 13. VCO circuit with 3 inverters

The parameter values of the MOS transistor models manufactured according to 65 nm design standards are shown in the following figure.

```
.MODEL N1 NMOS LEVEL=3 VTO=0.18 UO=160.000 TOX= 3.5E-9
+LD =0.005U THETA=0.300 GAMMA=0.400 RD=93 RS=143
+PHI=0.150 KAPPA=0.350 VMAX=180.00K
+CGSO=100.0p CGDO=100.0p L=65n W=650n
+CGBO= 60.0p CJSW=240.0p CBD=.61F CBS=.61F
* p-MOS Model 3:
.MODEL P1  PMOS LEVEL=3 VTO=-0.15 UO=120.000 TOX= 3.5E-9
+LD =0.005U THETA=0.300 GAMMA=0.400 RD=155 RS=155
+PHI=0.150 KAPPA=0.350 VMAX=180.00K
+CGSO=100.0p CGDO=100.0p L=65n W=1300n
+CGBO= 60.0p CJSW=240.0p CBD=.96F CBS=.96F
```

Figure 14. Parameters of the used MOS transistor models

A series of experiments allowed us to obtain the transfer characteristic of a VCO built on CMOS transistors with design standards of 65 nm, which is shown in Figure 15.

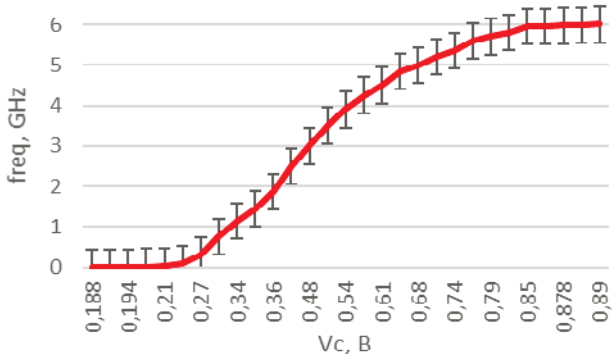


Figure 15. Transfer characteristic of VCO on 3 inverters

These simulation results were obtained with a supply voltage of Vcc = 0.9 volts. In addition, the dependence of the VCO output frequency on the supply voltage Vcc in the range of 0.25-2.5 volts was obtained, which is shown in Figure 16.

The final decision on the value of the Vcc supply voltage to be used should be made after the production of experimental samples, and this dependence can only serve as a guideline if it is necessary to increase the VCO output frequency.

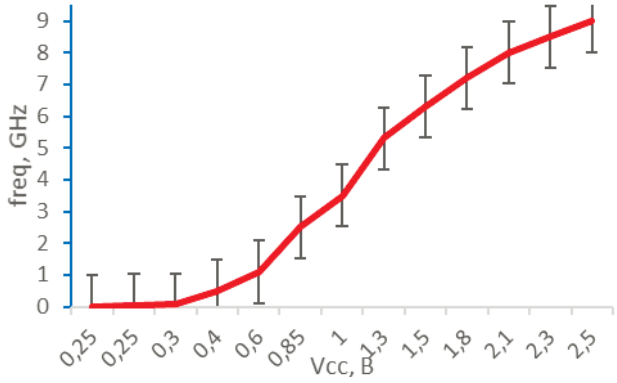


Figure 16. VCO output frequency versus supply voltage

The results obtained in this work show that the proposed circuit solutions can be used to create PLL devices for switching systems and data transmission control in high-performance quantum networks.

Conclusion

This paper examines some issues of creating a component base for quantum devices of optical data transmission systems. The principles of their technological production used for this purpose, some circuit solutions for creating such devices are shown, and the results of studies of the operability of the obtained devices are given, which indicate the possibility of implementing the necessary electronic component base for optical systems and other devices of various purposes.

In the future, the authors propose using the Cadence system for modeling, which will allow them to offer potential customers the results of modeling devices in the hardware description languages VHDL and VERILOG.

REFERENCES

[1] IEEE Journal on Selected Topics in Quantum Electronics. Vol: 29, Issue: 3: Photon. Elec. Co-Inte. and Adv. Trans. Print., May-June 2023.

[2] V. G. Fokin, R. Z. Ibragimov, “Optical systems with terabit and petabit transmission rates,”Textbook for universities. Moscow: Goryachaya Liniya – Telecom. 2017. 180 p.

[3] Dan M. Marom, Miri Blau, “Switching Solutions for WDM-SDM Optical Networks,” *IEEE Communications Magazine*. February 2015, pp. 60-68.

[4] M.G. Bakulin, T.B.K. Rejeb, V.B. Kreyndelin, Yu.B. Mironov, D.Y. Pankratov, A.E. Smirnov, "Modulation for cellular 5G/IMT-2020 and 6G networks," T-Comm, 2022. vol. 16, no.3, pp. 11-17. DOI: 10.36724/2072-8735-2022-16-3-11-17.

[5] M.G. Bakulin, V.B. Kreyndelin, D.Yu. Pankratov, "Application of MIMO technology in modern wireless communication systems of different generations," T-Comm, 2021. vol. 15, no.4, pp. 4-12. DOI: 10.36724/2072-8735-2021-15-4-4-12.

[6] Yong Soo Cho, Jaekwon Kim, Won Young Yang and Chung G. Kang, “MIMO-OFDM Wireless Communications with MATLAB,” John Wiley & Sons (Asia) Pte Ltd, 2010. 432 p.

[7] B. I. Shakhtarin, V. V. Sizykh, Yu. A. Sidorkina, I. M. Andrianov, K. S. Kalashnikov, “Synchronization in radio communication and radio navigation,” Moscow: Goryachaya Liniya – Telecom, 2011. 278 p.

[8] B. I. Shakhtarin, “Analysis of synchronization systems in the presence of interference,” Moscow: Goryachaya Liniya – Telecom, 2016. 360 p.

[9] A.V. Pestryakov, S.S. Dymkova, "Synchronization. 50 years development in the USSR and Russia," T-Comm, 2023. vol. 17, no.11, pp. 27-34. DOI: 10.36724/2072-8735-2023-17-11-27-34.

[10] A. L. Makarevich, M. S. Tokar, A. N. Kinash, V. A. Chubarov, “Analysis of the performance of PLL components in digital synchronization systems for high-speed applications,” *2018 Systems of synchronization, generation and processing of signals in telecommunications (SYNCHROINFO)*, July 2018, pp. 267-269.

[11] A. L. Makarevich, R. S. Gontsov, A. V. Kinash, N. I. Krasavtsev, Yu. V. Smelyanets, S. M. Sokovnich, “Study of characteristics of PLL system components for synchronization devices in high-speed data transmission networks,” *Problems of development of promising micro- and nanoelectronic systems (MES)*. 2020. Issue 2, pp. 147-152.

[12] A. L. Makarevich, S. M. Sokovnich, D. V. Garaga, L. I. Matyna, V. V. Sorochan, "Investigation of the Characteristics of Regulated Voltage Generators for PLL Systems and Frequency Synthesizers," *2022 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, 2022, pp. 1-5, doi: 10.1109/SYNCHROINFO 55067.2022.9840872.
[13] Etienne SICARD. Introducing 7-nm FinFET technology in Microwind. 2017. HAL Id: hal-01558775.https://hal.archives-ouvertes.fr/hal-01558775.
[14] V. Manassevich, “Frequency synthesizers. (Theory and design),” Moscow: Svyaz. 1979. 384 p.
[15] D. A. Balandin, A. D. Kuzmin, N. S. Surkov, “Analysis of the development of architectural solutions for frequency synthesizers,” *Problems of developing promising micro- and nanoelectronic systems (MES).* 2021. Issue 3, pp. 202-208.
[16] Alexander Chenakin, “Frequency Synthesizers: Concept to Product,” Norwood: Artech House, 2010.
[17] D. T. Spencer, T. Drake, T. C. Briles, J. Stone, L. C. Sinclair, C. Fredrick, S. B. Papp, “An optical-frequency synthesizer using integrated photonics,” Nature, 2018, no. 557(7703), pp.81–85.
[18] E. M. Savchenko, A. S. Budyakov, D. I. Garanovich, K. M. Ogurtsova, “Status and development prospects of integrated circuits of software-configurable radio frequency transceivers,” *Collection of works of the VIII All-Russian scientific and technical conference "Microwave Electronics and Microelectronics"*. St. Petersburg, 2019. Moscow: ETU "LETI" named after V.I. Ulyanov (Lenin), pp. 15-20.
[19] L. Sirleto, G. C. Righini, “An Introduction to Nonlinear Integrated Photonics: Structures and Devices,” *Micromachines* (Basel). 2023 Mar 7;14(3):614. doi: 10.3390/mi14030614. PMID: 36985020; PMCID: PMC10051308.
[20] Bruna Paredes, Zakria Mohammed, Juan Esteban Villegas, ”Ultra-compact ultra-wideband dual-mode transverse current-driven SWG multiplexer demonstrated at 64 Gbps,” *Lightwave Technology Magazine*. Vol.: 41, Issue: 16, August 15, 2023, pp. 5412-5417.
[21] N. K. Fontaine et al., “Few-Mode Fiber Wavelength Selective Switch with Spatial-Diversity and Reduced-Steering Angle,” OFC, OSA Tech. Digest (online), 2014, paper Th4A.7.
[22] L. E. Nelson et al., “Spatial Superchannel Routing in a Two-Span ROADM System for Space Division Multiplexing,” *J. Lightwave Tech*., vol. 32, no. 4, 2014, pp. 783-89.
[23] S. Y. Siew et al., “Review of silicon photonics technology and platform development,” *J. Lightw. Technol*., vol. 39, no. 13, pp. 4374-4389, Jul. 2021.
[24] A. L. Makarevich, V. V. Kulachek, S. M. Sokovnich, Ju. V. Zaharova, S. V. Zinchenko, “Analysis of the characteristics of synchronization system components for high-speed data networks,” *2024 Systems of Signals Generating and Processing in the Field of on Board Communications*, 12-14 March 2024, DOI:10.1109/IEEECONF60226.2024.10496786, p. 1-5.
[25] A. L. Makarevich, S. M. Sokovnich, V. V. Kulachek, S. V. Zinchenko, Y. V. Zaharova, "Analysis of the State of Development of the Component Base for Quantum Devices of Optical Data Transmission Systems," *2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, 01-03 July 2024, DOI:10.1109/SYNCHROINFO61835.2024.10617462, pp. 1-7.
[26] A. L. Makarevich, D. V. Garaga, S. M. Sokovnich, N. S. Kostyukevich, S. A. Karapetyan, “Circuit Design of a Frequency Synthesizer Device for High-Speed Data Transmission Systems,” *Systems of Signals Generating and Processing in the Field of on Board Communications*, 2022, pp. 1-4, doi: 10.1109 / IEEE CONF 53456. 2022. 9744274.
[27] F. M. Gardner. “Phaselock Tekniquis”, Third Edition. John Wiley & Sons, Inc., 2005, 422 p.
[28] Zhong Gao, Robert Bogdan Staszewski, Masoud Babaie, "Canceling Fundamental Fractional Spurs Due to Self-Interference in a Digital Phase-Locked Loop," *IEEE Journal of Solid-State Circuits.* Vol. 59, Issue 11, November 2024, pp. 3716-3729, DOI: 10.1109/JSSC.2024.3393478.
[29] Sehyun Jang, Moonjae Chae, Park Hangi, Changwoong Hwang, Jaehyuk Choi, "A Low-Jitter and Compact-Area Fractional-N Digital PLL with Fast Multi-Variable Calibration Using the Recursive Least-Squares Algorithm," *IEEE Journal of Solid-State Circuits*. Vol. 59, Issue 12, December 2024, pp. 3884-3897, DOI:10.1109/JSSC.2024.3456105

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

NOISY SPEECH COMMANDS RECOGNITION ALGORITHM BASED ON TEST SPECTRAL TRANSFORMATIONS OF INPUT SIGNAL

Chi Thien Nguyen [1]

[1] Ho Chi Minh City University of Technology (HCMUT), Ho Chi Minh City, Vietnam

ABSTRACT

In practice, the result of signal recognition is degraded by noise. Training speech signals are usually noise-free, while testing speech signals are noisy. The presence of noise leads to a strong deviation of the spectra of the testing speech signals from the spectra of their standards in the training sample. Therefore, the quality of the recognition result against a background of noise drops sharply. The article proposes a trial amplification of the speech signal spectrum in the recognition process. A multiple algorithm for recognizing commands against a background of noise is compared with a single algorithm for recognizing speech commands. The problem of recognition of speech commands on the background noise is reviewed. The developed numerical algorithm of recognition is studied. The results of the experiments are reported on 11 speech commands from the TIDigits dataset.

KEYWORDS: *recognition of speech commands, noise, multiple algorithm*

DOI: 10.36724/2664-066X-2024-10-5-16-21

Received: 25.07.2024
Accepted: 14.09.2024

Citation: Chi Thien Nguyen, "Noisy speech commands recognition algorithm based on test spectral transformations of input signal" *Synchroinfo Journal* **2024**, vol. 10, no. 5, pp. 16-21

Introduction

In practice, the speech signals recognition [1-6] result is degraded by noise. Training speech signals are usually noise-free, while testing speech signals are noisy. The presence of noise leads to a strong deviation of the spectra of the testing speech signals from the spectra of their standards in the training sample. Therefore, the quality of the recognition result against a noise background drops sharply [7]. In [7], to solve the problem of recognizing speech commands against a noise background, it is proposed to amplify the signal spectrum by a constant. This means that the values of the signal amplitude spectrum samples are increased by a constant. In [8], algorithms were proposed for determining optimal gain constants for each application condition and a single gain constant for different application conditions. The positive results of these studies confirm the improvement in recognition quality by amplifying the signal spectrum. This raises an important question about what to do if we do not have any a priori information about the noise (noise type, noise level).

Command recognition against a noise background.

A trial amplification of the speech signal spectrum during the recognition process is proposed. When executing the algorithm for recognizing speech commands against a noise background in [7], the speech signal is transformed with a fixed value of the gain constant c. We will call such an algorithm a single-shot recognition algorithm. If a trial transformation of the speech signal during the recognition process is taken into account, i.e. the constant c can change, then the algorithm for recognizing speech commands against a noise background becomes multiple. The steps of the multiple algorithm for recognizing speech commands against a noise background (MARSC) are given below:

1. Construct a sequence $A = (a_1, a_2, a_3,...)$ of short-term spectra [9] $\mathbf{a}_i$ ($a_i^k, 1 \le k \le N/2$) from a speech signal $Y = (y_1,..., y^T)$.

2. Take one value of the gain constant c from a predetermined range [0, 0.1,..., 1.9]. Increase the values of the amplitude spectra by the next value of the constant c. After "amplifying" the short-term amplitude spectrum by $c \ge 0$, a new sequence of amplitude spectra is obtained $\tilde{A} = \{\tilde{\mathbf{a}}_1, \tilde{\mathbf{a}}_2, \tilde{\mathbf{a}}_3, ...\}$, where $\tilde{\mathbf{a}}_i = \{\tilde{\mathbf{a}}_i^k, 1 \le k \le N/2\}$, $\tilde{a}_i^k = \tilde{a}_i^k + c$.

3. Obtain a sequence $X = (x_1, x_2, x_3,...)$ of vectors of small-frequency cepstral coefficients [9] $\mathbf{x}_t$ ($x_t^m, 1 \le m \le M$) from the sequence $\tilde{A} = \{\tilde{\mathbf{a}}_1, \tilde{\mathbf{a}}_2, \tilde{\mathbf{a}}_3, ...\}$, of short-term amplitude spectra.

4. Calculate the probability $p(X(c) \mid \lambda^v(c))$ of the sequence vectors X mel-frequency cepstral coefficients with respect to each signal class $v = 1,2,...,V$, where the parameter $\lambda^v(c)$ describes the v-th signal class after amplifying their spectrum by a constant c. In the database, each signal class $v = 1,...,V$ describes a set of standards $\lambda^v(c)$ with different levels of amplification of signal spectra $c \in [0, 0.1,..., 1.9]$..

5. Repeat teps 2-4 for all values of the constant c.

6. Among all set (c, v), find the set (c^*, v^*) that provides the maximum probability $p(X(c) \mid \lambda^v(c))$.

Thus, the corresponding number v* of the signal class is:

$$v^* = \arg \max_c \max_{\lambda^v} p(X(c) \mid \lambda^v(c)), \; v = 1,2,...,V.$$

Thus, when executing the MARKS algorithm, some value of the gain constant c is selected from the range [0, 0.1,..., 1.9]. In the general case, the use of some value of the gain constant c from this range does not mean at all that the mel-frequency cepstral representation of the input signal becomes closer to the mel-frequency cepstral representation of the reference signals. But, ultimately, such an optimal value of the gain constant c will be selected that will still improve the quality of recognition of the input signal, which means approaching the mel-frequency cepstral representation of the reference signals.

Algorithm study for recognizing commands against a noise background

A comparison of the multiple-shot command recognition algorithm against a background of noise MARKS and the single-shot speech command recognition algorithm (CRA) is performed. The CRA algorithm is a variant of the MARKS algorithm with the gain constant c = 0. Experiments were conducted on 11 speech commands from the TIDigits dataset [10-13]. The set of 440 speech signals from 40 speakers is randomly divided into two samples (each sample contains signals from 20 speakers who pronounced each command once). One sample plays the role of a training sample, the other is used as a test sample. The training sample is used to train the MARKS and CRA algorithms. Noise with a signal-to-noise ratio of R_{sn} (dB) was artificially added to the test speech signals.

For a given speech signal $\Psi = \{\psi_1,...,\psi_T\}$ and noise $\Xi = \{\xi_1,...,\xi_T\}$ with value R_{sn}, the noisy speech signal $Y = \{y_1,..., y_T\}$ is formed by the formula [14].

$$y_t = \psi_t + 10^{-\frac{R_{sn}}{20}} \xi_t \sqrt{\sum_{i=1}^{T} \psi_i^2 / \sum_{i=1}^{T} \varsigma_i^2}, \quad t = 1,...,T.$$

The recognition of speech signals contaminated with additive white Gaussian noise is considered. Figure 1 shows additive white Gaussian noise and its amplitude spectrum. For example, for additive white Gaussian noise with a noise level of R_{sn} = 6.9,12,15 dB for the model of signal classes as two-component random processes, recognition is performed by the MARKS and CRA algorithms with the number of recognition errors counted. Figure 2 shows the recognition result.

It turned out that for additive white Gaussian noise with a noise level of R_{sn} = 6.9,12,15 dB, on average, the use of the MARKS algorithm leads to a decrease in the number of recognition errors compared to the use of the CRA algorithm by 51.59%.

The recognition of speech signals contaminated with real environmental noise from the exhibition hall is considered [15].

Figure 3 shows the ambient noise from the exhibition hall and its amplitude spectrum. For example, for ambient noise from the exhibition hall with a noise level of R_{sn} = 6.9,12.15 dB, for the model of signal classes as two-component random processes, recognition is performed by the MARKS and CRA algorithms with the number of recognition errors counted. Figure 4 shows the recognition result. It turned out that for ambient noise from the exhibition hall with a noise level of R_{sn} = 6.9,12.15 dB, on average, the use of the MARKS algorithm leads to a decrease in the number of recognition errors compared to the use of the CRA algorithm by 31.25%.

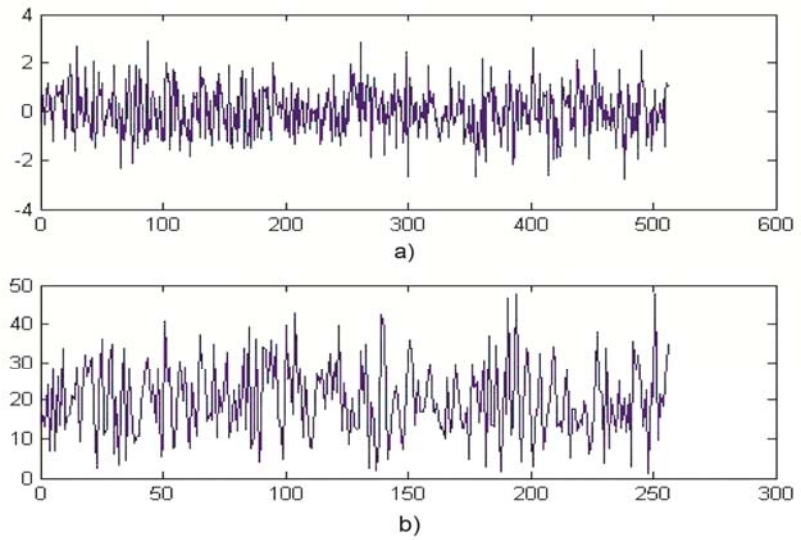


Figure 1. Additive white Gaussian noise a) and its amplitude spectrum b)

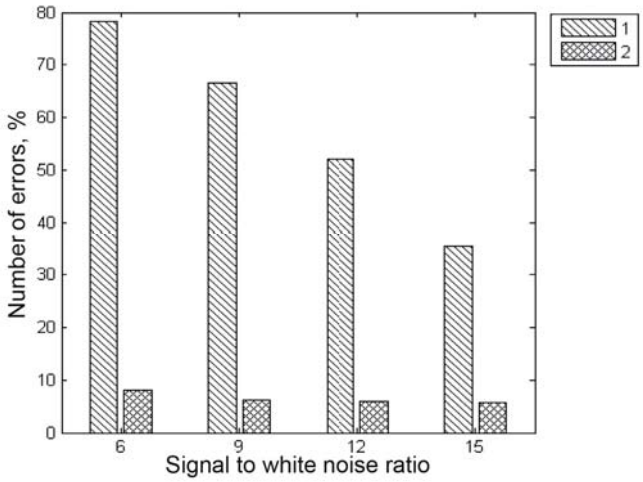


Figure 2. Number of recognition errors by algorithms: 1 – CRA; 2 – MARKS

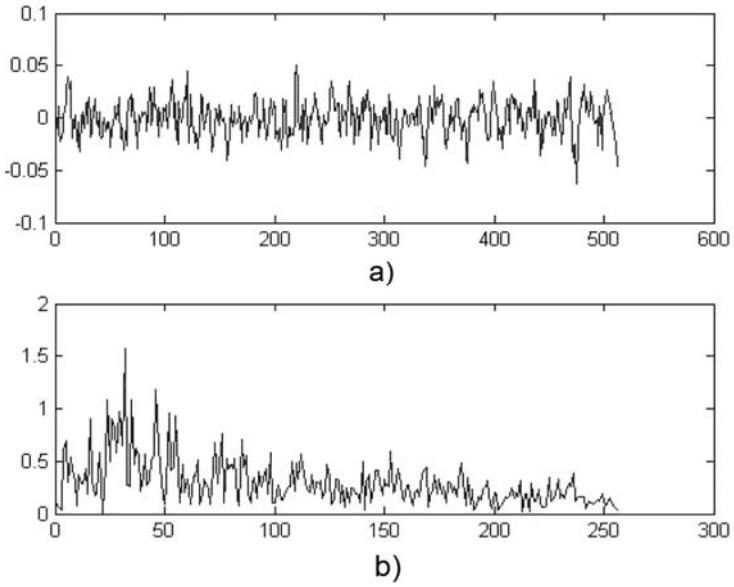


Figure 3. Ambient noise from the exhibition hall a), and its amplitude spectrum b)

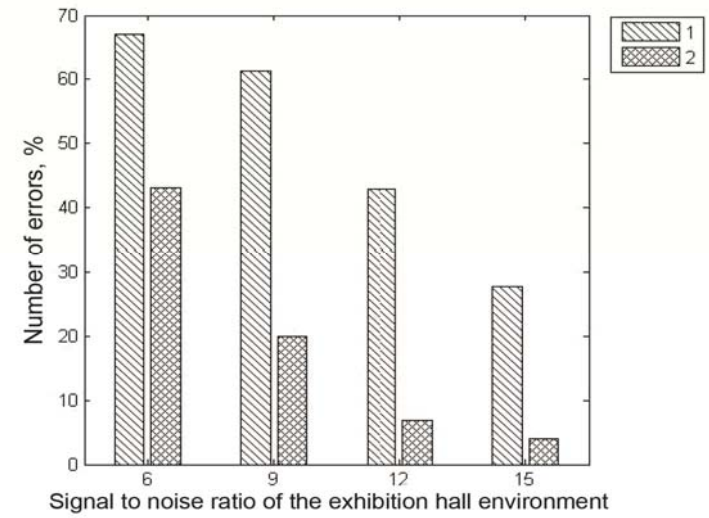


Figure 4. Number of recognition errors by algorithms: 1 – CRA; 2 – MARKS

Recognition of speech signals contaminated with real noise inside a moving subway train is also considered [15].

Figure 5 shows the noise inside a moving subway train and its amplitude spectrum.

As a conclusion after analyzing the literature, it can be said that multiplexers and demultiplexers are the basis for creating switches that control the flow of transmitted information in optical systems, while the synchronicity of their operation will be ensured by PLL devices implemented as part of specialized microcircuits manufactured using CMOS technology with submicron design standards.

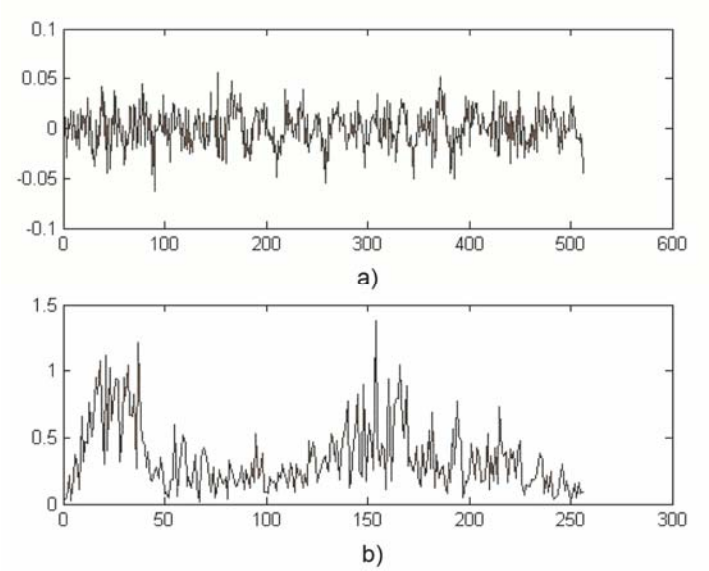


Figure 5. Noise inside a moving subway train a), and its amplitude spectrum b)

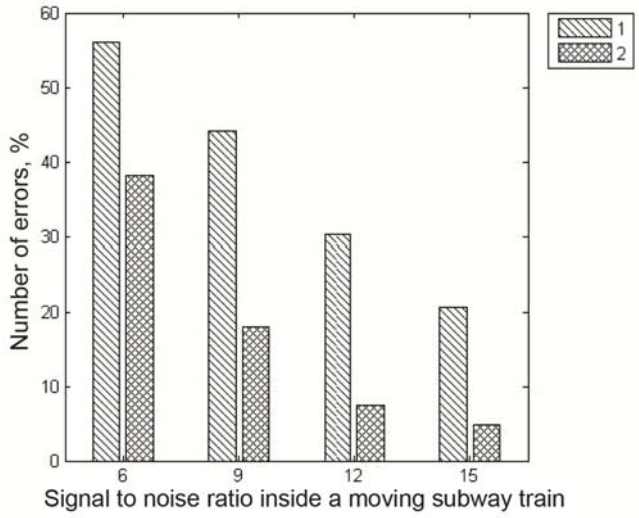


Figure 6. Number of recognition errors by algorithms: 1 – CRA; 2 – MARKS

For example, for the noise inside a moving subway train with a noise level of R^{sn} = 6.9,12.15 dB, for the model of signal classes as two-component random processes, recognition is performed by the MARKS and CRA algorithms with the number of recognition errors counted. Figure 6 shows the recognition result.

It turned out that for the noise inside a moving subway train with a noise level of R_{sn} = 6.9,12.15 dB, on average, the use of the MARKS algorithm leads to a decrease in the number of recognition errors compared to the use of the CRA algorithm by 20.68%.

Thus, the experiments show that the MARKS algorithm effectively improves the quality of speech command recognition against a noise background.

REFERENCES

[1] G. K. Berdibayeva, A. N. Spirkin, O. N. Bodin and O. E. Bezborodova, "Features of Speech Commands Recognition Using an Artificial Neural Network," *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, Yekaterinburg, Russia, 2021, pp. 0157-0160, doi: 10.1109/USBEREIT51232.2021.9455111.

[2] Daniel-S. Arias-Otalora, Andrés Florez, Gerson Mellizo, C. H. Rodríguez-Garavito, E. Romero, J. A. Tumialan, "A Machine Learning Based Command Voice Recognition Interface", *Applied Computer Sciences in Engineering*, vol.1685, pp.450, 2022.

[3] A. R B, V. R C, V. K, S. Chikamath, N. S R and S. Budihal, "Limited Vocabulary Speech Recognition," *2024 3rd International Conference for Innovation in Technology (INOCON)*, Bangalore, India, 2024, pp. 1-5, doi: 10.1109/INOCON60754.2024.10511500.

[4] A. Kuzdeuov, S. Nurgaliyev, D. Turmakhan, N. Laiyk and H. A. Varol, "Speech Command Recognition: Text-to-Speech and Speech Corpus Scraping Are All You Need," *2023 3rd International Conference on Robotics, Automation and Artificial Intelligence (RAAI)*, Singapore, Singapore, 2023, pp. 286-291, doi: 10.1109/RAAI59955.2023.10601292.

[5] Aditya Kulkarni, Vaishali Jabade, Aniket Patil, "Audio Recognition Using Deep Learning for Edge Devices", *Advances in Computing and Data Sciences*, vol.1614, pp.186, 2022.

[6] A. Yasmeen, F. I. Rahman, S. Ahmed and M. H. Kabir, "CSVC-Net: Code-Switched Voice Command Classification using Deep CNN-LSTM Network," *2021 Joint 10th International Conference on Informatics, Electronics & Vision (ICIEV) and 2021 5th International Conference on Imaging, Vision & Pattern Recognition (icIVPR)*, Kitakyushu, Japan, 2021, pp. 1-8, doi: 10.1109/ICIEVicIVPR52578.2021.9564183.

[7] C. T. Nguyen, “Solution of the problem of speech command recognition against a noise background,” *Bulletin of Tula State University. Technical sciences*. Issue 11. Tula: Tula State University Publishing House, 2013, pp. 241-250.

[8] C. T. Nguyen, “Optimization of the parameters of the heuristic model of speech signals in order to improve the quality of their recognition,” *Bulletin of Tula State University. Technical sciences*. 2014. Issue 1, pp. 44-50.

[9] J. Benesty et al., “Handbook of speech processing.” Springer, 2008. 1159 p.

[10] G. Leonard, G. Doddington, TIDigits [Electronic resource]. Linguistic Data Consortium, Philadelphia, 1993. URL: https://catalog.ldc.upenn.edu/LDC93S10 (date of access: 23.03.2024).

[11] H. Aghakhani et al., "Venomave: Targeted Poisoning Against Speech Recognition," *2023 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)*, Raleigh, NC, USA, 2023, pp. 404-417, doi: 10.1109/SaTML54575.2023.00035.

[12] L. Guo et al., "Transformer-Based Spiking Neural Networks for Multimodal Audiovisual Classification," *IEEE Transactions on Cognitive and Developmental Systems*, vol. 16, no. 3, pp. 1077-1086, June 2024, doi: 10.1109/TCDS.2023.3327081.

[13] S. Xiang et al., "Neuromorphic Speech Recognition with Photonic Convolutional Spiking Neural Networks," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 29, no. 6: Photonic Signal Processing, pp. 1-7, Nov.-Dec. 2023, Art no. 7600507, doi: 10.1109/JSTQE.2023.3240248.

[14] K. Wojcicki, “Add noise to a signal at a prescribed SNR level,” URL: http://www.mathworks.com/matlabcentral/ (date of access: 10.03.2024).

[15] http://labrosa.ee.columbia.edu/sounds/noise/ (date of access: 15.03.2024).

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

ELECTROMAGNETIC COMPATIBILITY BETWEEN 4G/5G MOBILE COMMUNICATIONS AND RAILWAY TELECOMMUNICATION EQUIPMENT

Aliaksandr Svistunou, Vladimir Mordachev, Eugene Sinkevich [1, 2]

[1] China-Belarus Belt and Road joint Laboratory on Electromagnetic Environment Effect;

[2] Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus

emc@bsuir.by, mordachev@bsuir.by, esinkevich@bsuir.by

ABSTRACT

Modern railway transport and infrastructure require modern communication systems. Railway transport control systems are complex critically important informatization objects and have several control levels: operation, centralization and element control. Today, the transport industry is gradually mastering the next generation of technological radio communications based on LTE (Long-Term Evolution) and 5G technologies. The development of telecommunication systems in railway transport allows improving the quality of services provided to passengers and ensuring a higher level of safety thanks to remote monitoring used to promptly identify and resolve emergency situations. However, it is difficult to find optimal solutions now, due to the large number of communication nodes, difficult operating conditions, electromagnetic interference and limited space. In this work a systems analysis of electromagnetic compatibility of 4G/5G mobile communication equipment and railway equipment is performed. Unified criteria for the stability of railway signaling and telecommunications equipment to radio frequency electromagnetic influence through housing ports are used. A statistical approach is applied based on the analysis of the conditionally average level of electromagnetic background generated by 4G/5G base stations. The worst estimate of the required spacing of 4G/5G equipment and railway equipment providing their EMC is also applied. The analysis results show a significant potential hazard of radiation from 4G/5G base stations and subscriber equipment, underestimation of which is fraught with catastrophic consequences. Possible ways to eliminate the risk of disruption of railway signaling and telecommunications equipment in a complex electromagnetic environment created by 4G/5G systems are discussed.

KEYWORDS: *4G/5G systems, mobile communications, railway signaling, electromagnetic exposure*

DOI: 10.36724/2664-066X-2024-10-5-22-32

Received: 25.07.2024
Accepted: 14.09.2024

Citation: Aliaksandr Svistunou, Vladimir Mordachev, Eugene Sinkevich, "Electromagnetic Compatibility between 4G/5G Mobile Communications and Railway Telecommunication Equipment" *Synchroinfo Journal* **2024**, vol. 10, no. 5, pp. 22-32

Licensee IRIS, Vienna, Austria.

Introduction

The massive use of electronics and wireless technologies in all infrastructures of modern society without a timely solution of the emerging EMC problems of the shared equipment of various infrastructures can cause conflicts between them. Such conflicts are especially acute at the explosive nature of the expansion of the use of wireless technologies in a separate infrastructure. Today, the most rapidly expanding is information infrastructure which encompasses mobile communication (MC) systems and networks. During the 4G-5G-6G evolution of MC, the change of MC generations every 10 years is accompanied by a tenfold increase in the quantity of sources of radio-frequency electromagnetic radiation, a hundredfold increase in the area traffic capacity (mobile traffic area density) and data rates over radio channels with a corresponding increase in broadbandness and the complication of the time-frequency structure of MC radiations, as well as a significant expansion of the used frequency range [1, 2].

For example, a big plus of 5G is that passengers do not have to spend money on paid Wi-Fi. If you focus on 5G, then the carrier does not have to do anything at all - just wait until mobile operators install 5G base stations along the railway tracks. Then carry out an inexpensive upgrade of train modems that receive a signal from mobile operators, from LTE to 5G and power the on-board Wi-Fi network with this traffic. The weak point of this strategy is that 5G equipment along the railway appears only on very popular and short routes.

5G inherits the general disadvantage of cellular communications in the form of a drop in bandwidth when registering a large number of subscribers in a cell. Another disadvantage is the growing latency when registering a smartphone in the cell of the next base station as the train picks up speed. Accordingly, the speed of the Internet connection on the device will drop. Already for a speed of 100 km / h, the connection degradation will be about 30%. It is expected that for high-speed trains (250-400+ km/h), the quality of communication via a cellular channel will be even worse. It is worth noting the asymmetric nature of 5G communication, when the download speed for all operators is approximately 20 times higher than the upload speed. This drawback, especially in trains, is difficult to eliminate due to the physics of the process. The base station has a powerful transmitter, so the signal can have a complex modulation form to ensure a broadband connection. The smartphone transmitter, on the contrary, is low-power and works from inside the metal body of the car, so a simpler modulation scheme is forced to be used (usually at the level of data speed for 4G-3G), so that the base station can receive a weak signal from the subscriber. These shortcomings are not critical in themselves, but in total they give a negative synergistic effect. A modern train has a large number of digital systems, the most important of which is real-time video surveillance and online transmission of images from the driver's cabin and from cameras in the cars to the traffic control center. This allows for machine facial recognition to prevent criminal and terrorist activity on trains, as well as to quickly respond to various emergency situations (fire, derailment, etc.). Communication interruptions for remote video surveillance are unacceptable, and 5G's capabilities in terms of outgoing traffic (upload) are too weak to transmit video streams from multiple HD cameras.

All this causes a very significant complication of the electromagnetic environment (EME), especially in places with a high population density and economic activity, which can cause disruption of the operation of the technical systems of other infrastructures. This is confirmed in works [3-5], which proved the potential danger of interference from base stations (BS) and user equipment (UE) of 4G/5G MC for healthcare infrastructure equipment. Therefore, an important task is to analyze the EMC of 4G/5G MC equipment and technical systems of other infrastructures of modern society.

Modern railway control systems are among the critically important objects of informatization; they are complex and have several control levels: the operation control level, the interlocking (centralization) level, and the element control level. The widespread use of wired and wireless communication, microprocessor interlocking, signaling, and auto-blocking in these systems, which unlike electromechanical equipment has a significantly higher susceptibility to radio-frequency electromagnetic fields (EMF), causes the need to analyze and ensure the reliability of operation of modern railway signaling systems, railway communication & data transmission systems and microelectronic systems for ensuring the safety of train traffic in the context of the rapid EME complication due to the extremely intensive development of wireless technologies and 4G/5G MC.

The objective of this paper is to perform a system-level analysis of EMC between the 4G/5G MC equipment and the railway equipment, namely to estimate a danger of interference from BS and UE of 4G/5G MC to the railway signaling and telecommunication equipment.

EMC analysis of railway and 4G/5G equipment

1) The EMC analysis for railway equipment and MC 4G/5G radio equipment have been performed using exposure limits – maximum permissible levels (MPL) of EMFs in various frequency bands specified by current standards [6-8] and typical data [9-16] for parameters of 4G/5G BS and UE radiations.

2) The alysis of the EMC conditions of the specified equipment was carried out by calculating the required spatial separation between them for the case of free-space radio wave propagation – the minimum distance at which the EMF level of the MC equipment affecting the railway equipment is equal to MPL.

3) Integral assessments of the danger created in the places of operation of railway equipment by MC radiations were made by system analysis technique [17, 18] of the conditional average intensity of the electromagnetic background (EMB) created by the set of BS radiations near the earth's surface during the implementation of separate 5G scenarios.

Immunity of railway equipment to electromagnetic field

Table 1 lists the requirements [6-8] for the immunity of railway signaling and telecommunication equipment (critical railway equipment, the requirements for the immunity of which to the EMF exposure are standardized for EMFs penetrating into this equipment through the enclosure ports).

Table 1

Requirements for the Immunity of Railway Signaling and Telecommunication Equipment to EMF

Frequency band, MHz	MPL, V/m	Ref.
80–800 (Environmental phenomena is radiofrequency EMF, amplitude modulated [7])	10	[6], [7]
800–1000 1400–2000 2000–2700 5100–6000 (Environmental phenomena is radiofrequency EMF, from digital communication devices [7])	20 10 5 3	[6], [7]
2700–6000	3	[8]

It should be noted that the requirements [6-8] for the MPLs of EMFs affecting this railway equipment are defined only for a few sections of the FR1 5G frequency range, and are completely absent for the FR2 5G range. The question of the susceptibility of this railway equipment to EMFs at all frequencies of FR1 & FR2 ranges remains open, as well as the question of the influence on this susceptibility of the complication of the frequency-time structure of 4G/5G MC radiations; this may pose a great potential danger to railway transport in the future.

Required spacing of railway and 4G/5G equipment

The required distance between the railway and MC equipment for the case of free-space radio wave propagation is calculated by using the following expression:

$$d = \sqrt{30P_{EIRP}} \big/ E_{MPL} \text{ , m} \quad (1)$$

where E_{MPL} is the EMF MPL, [V/m]; P_{EIRP} is the equivalent isotropic radiated power (EIRP) of the MC equipment, [W].

Tables 2 and 3 show the results of calculating the required spatial separation between the 4G/5G MC and the considered railway equipment.

In these calculations, the following data for the BS and UE characteristics of 4G/5G MC that determine their EIRP were used:

a) The adjustable output power of an outdoor BS transmitter can reach 43–53 dBm [9, 10], the BS antenna gain is 12–40 dB [11–14]. Thus, the range of EIRP values in the main lobes of BS antenna patterns from 0.1 to 100 kW is of interest for analysis.

b) UE maximum output power is 25 dBm for LTE FDD UE, 28 dBm for LTE TDD UE, and 29 dBm for 5G UE taking into account the requirement to the tolerance; UE antenna gain is 0 dBi [15, 16].

Table 2

Required spatial separation between BS with different EIRP and railway equipment

EIRP, kW	***E*$_{MPL}$, V/m**			
	3	**5**	**10**	**20**
	Required separation, m			
0.1	18.3	11	5.5	2.7
0.5	40.8	24.5	12.3	6.1
1	57.7	34.6	17.3	8.7
5	129	77.5	38.7	19.4
10	183	110	54.8	27.4
20	258	155	77.5	38.7
40	365	219	110	54.8
60	447	268	134	67.1
80	516	310	155	77.5
100	577	346	173	86.6

Table 3

Required spatial separation between UE and railway equipment

EIRP, dBm	***E*$_{MPL}$, V/m**			
	3	**5**	**10**	**20**
	Required separation, m			
25	1,03	0.62	0.31	0.15
28	1,45	0.87	0.44	0.22
29	1.63	0.98	0.49	0.24

Intensity of electromagnetic background created by base-station radiations

Estimates of the conditional average intensity of EMB created by MC radio networks according to the technique [17, 18] are based on determining the average electromagnetic loading on area (EMLA) created by the radiations of BS and UE located in the considered territory, which is proportional to the average AREA TRAFFIC CAPACITY , reaching 10^5 bit/s /m^2 in 4G networks and 10^7 bit/s/m^2 in 5G networks [1]. Since a data transmission mode with a significant asymmetry of uplink and downlink traffic is dominated in 4G/5G networks, the contribution of radiations of many UEs to the total EMB intensity created by 4G/5G MC systems turns out to be insignificant. This allows us to limit to considering only the EMB component near the earth's surface generated by BS radiations.

The EMB intensity Z_Σ [W/m^2] in a certain observation point is determined as a scalar sum of power flux densities Z_n of EMFs generated by a set of N sources located in the area S of their radio visibility from the observation point:

$$Z_\Sigma = \sum_{n=1}^{N} Z_n, \quad Z_n \geq Z_0, \tag{2}$$

where Z_0 is the threshold of EMF sources radio visibility from the observation point. Due to the known properties of EME created by spatially distributed EMF sources, the value of Z_Σ is determined by a predominant components in (2).

Estimations of the total averaged intensity $Z_{\Sigma BS}$ of EMB in the corresponding frequency band, created in the observation point by radiations of the set of BS, located uniformly randomly with respect to the observation point in all area of BS radio visibility from the observation point, can be made using the following expression:

$$Z_\Sigma \approx \frac{B_{TBS}}{2} ln\left(\frac{4\sqrt{e}H_{OP}}{\lambda}\right), \quad H_{OP} \geq \frac{\lambda}{4}. \tag{3}$$

In this expression, λ [m] is the wavelength; H_{OP} [m] is the height of the observation point over the earth's surface, note that H_{OP} is much less then the heights of BS antennas; B_{TBS} [W/m^2] is the EMLA created by BS radiations and has the meaning of the average area density of the total power of their EMFs reaching the earth's surface.

The technique developed in [17, 18] for estimating the average EMLA B_{TBS} is based on the analysis of the level S_{tr} [bit/s/m^2] of area traffic capacity near the earth's surface created by BS radiations. Great growth of area traffic capacity is declared in [1, 2]. In this case, the expression for estimating the average EMLA has the following form:

$$\left.\begin{aligned} B_{TBS} &\approx \frac{8\pi^2 kT_0 mK_N K_S L_P SNIR\left(K_{CC}+1\right)R_{max}^2 S_{tr}}{\lambda^2 G_0 \log_2\left(1+SNIR\right)}, \\ SNIR &= \left(2^{mS_{ER}}-1\right). \end{aligned}\right\} \tag{4}$$

In this expression G_0 is the BS antenna gain, R_{max} is the radius of the BS service area, k is the Boltzmann's constant, 1.38×10^{-23} J/C; K_N is the UE receivers noise factor; T_0 is the ambient temperature; K_S is a coefficient characterizing the necessary margin in the level of the signal received by UE, for the implementation of system-forming functions (handover, etc.); L_P is the necessary margin for BS radiation power to overcome the additional radio wave propagation losses in relation to the free space, caused by the attenuation of radio waves at the entrance to buildings, their fading in the "canyons" of urban development and other factors; K_{CC} characterizes the excess by the intra-network interference of the UE

receiver's internal noise; S_{ER} [bit/s/Hz] is the real spectral efficiency of data transfer through BS radio channels, $m \geq 1$ is a coefficient characterizing how many times the radio channel real spectral efficiency is lower than the potential one (or higher when using MIMO technology, in this case may be $m<1$); *SNIR* – the ratio of UE input signal power to the total power of intrasystem interference and UE receiver's internal noise on its input.

Intensity of electromagnetic background for basic 5G EMBB scenarios

The figures given below show the calculated dependences of the average EMB intensity generated by the BS radiations on the area traffic capacity level, for typical radio reception parameters $K_N=5$, $T_0=290$K. Since in MC radio channels without MIMO $m \approx 2...10$, and the planned increase in the spectral efficiency of 4G/5G radio channels due to MIMO technology is 2-8 times [19], it is actually only compensates for the imperfection of the modulation/demodulation and encoding-decoding processes; therefore, it is advisable to perform estimations of the intensity of EMB created by 4G/5G MC, using (3),(4) for $m=1$, assuming that the data transfer rate in radio channels of these systems is close to the potential).

We restrict to the analysis of three basic 5G eMBB scenarios recommended by [20] that create the highest EMB levels. The calculated data presented below in graphical form were obtained for typical values of the parameters included in (4). In the figures below, four lower dotted horizontal lines (green) indicate the EMF MPL values for railway equipment that comply with the standards [6–8] (see Table 1), the upper dotted line (red) indicates the MPL 1000 μW/cm^2 recommended by [21] for people electromagnetic protection, taking into account the danger of the thermal damage of biological tissues when exposed to radio frequency EMFs.

Figure 1 corresponds to the "Dense Urban eMBB" 5G scenario, the intersite distance in which is 200 m (R_{max} = 100 m), the dependences $Z_\Sigma(S_{TR})$ of the conditional average EMB intensity on the area traffic capacity level were obtained for various frequencies of the 5G FR1 range (0.41–7.125 GHz). Their analysis allows us to conclude that already at S_{TR} = 10^5 bit/s/m^2, corresponding to the 4G limit, the generation of this traffic at frequencies above 2 GHz makes the EME created in this case potentially dangerous for railway equipment, and the increase of the area traffic capacity to the level of 10^6–10^7 bit/s/m^2 declared for 5G MC increases the intensity of created EMB by 1-2 orders of magnitude – to levels 2-3 orders of magnitude higher than EMF MPLs for railway equipment.

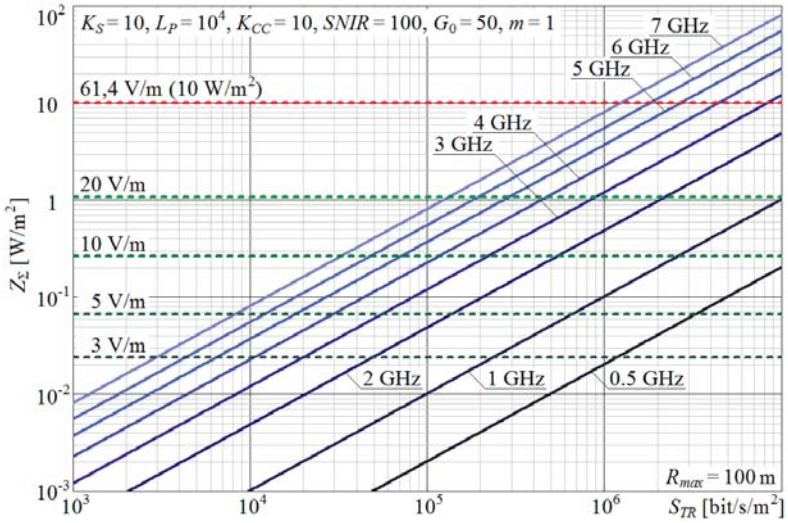


Fig. 1. Dependences of conditional average intensity of electromagnetic background created in 5G scenario "Dense Urban eMBB" on area traffic capacity for various frequencies in FR1 range

Figure 2 corresponds to the "Rural eMBB" 5G scenario, corresponding to the implementation of eMBB services in rural areas with a terrestrial density of UE that is 2 orders of magnitude lower than in the previous scenario; the intersite distance in this case was 2000 m (R_{max} = 1000 m). $Z_\Sigma(S_{TR})$ dependences were obtained for the same frequencies of the 5G FR1 range. Analysis of these dependences shows that already at an average area traffic capacity of 10^3 bit/s/m^2, which is 2 orders of magnitude lower than the limit declared for 4G systems, the EMB levels created by MC systems turn out to be comparable to EMF MPLs for the considered railway equipment, and with an increase in area traffic capacity to levels of $10^4 – 10^5$ bit/s/m^2, expected during the full-scale implementation of eMBB services in rural areas, the conditional average intensity of the created EMB is also capable of exceeding these EMF MPLs by 2-3 orders of magnitude.

Figure 3 corresponds to the "Hotspot eMBB" 5G scenario using frequencies of the 5G FR2 range (24.25–52.6 GHz with extension up to 70-100 GHz). Calculations were performed as for the basic “budget” version [20] using BS (access points) with weakly directional radiation (4 upper graphs), and for a promising version with multi-element active phased array antennas (APAA) with directional radiation in the "Beamforming" mode (4 lower graphs). This scenario is focused on implementation in areas of intensive use of MC wireless services both indoors (Indoor Hotspot) and in places where UEs are locally concentrated outdoors (Outdoor Hotspot), in particular, in places where passengers are concentrated (railway platforms, etc.).

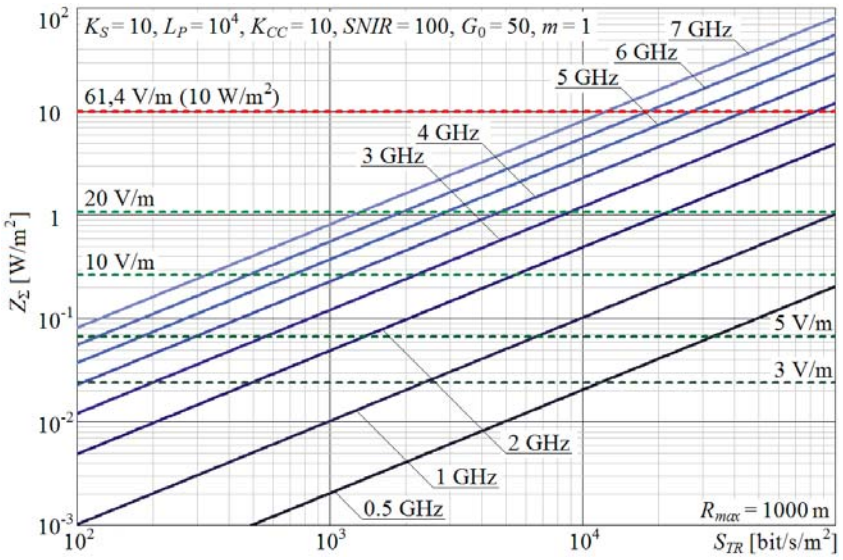


Fig. 2. Dependences of conditional average intensity of electromagnetic background created in 5G scenario "Rural eMBB" on area traffic capacity for various frequencies in FR1 range

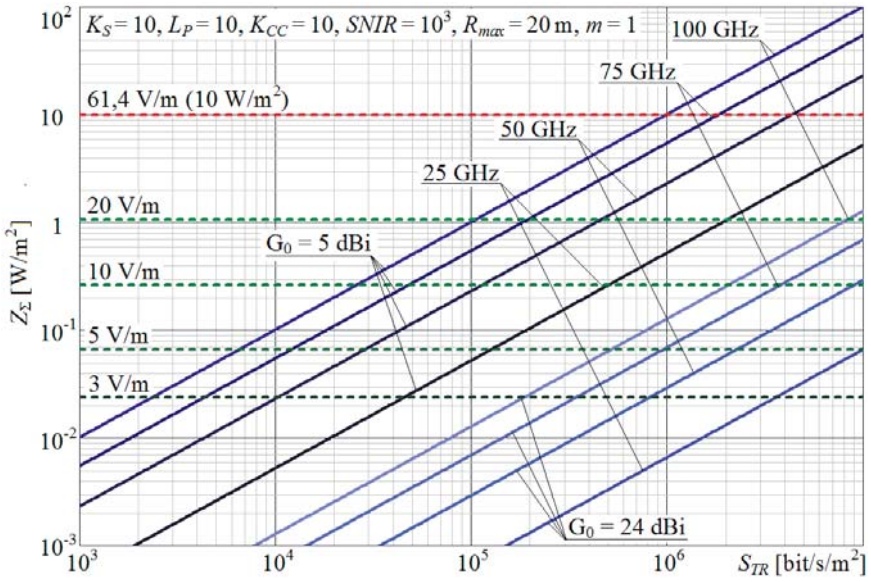


Fig. 3. Dependences of conditional average intensity of electromagnetic background created in 5G scenario "Indoor/Outdoor Hotspot eMBB" on area traffic capacity for various frequencies in FR2 range and different gain of 5G base station antennas

Analysis of dependences given in Figure 3 allows us to conclude that when using low-directional antennas in this scenario, already at average area traffic capacity level 10^5 bit/s/m^2, corresponding to the 4G limit, the location of railway equipment at distances up to 10-20 m from the BS can be dangerous, but since EMF MPLs for the FR2 range is not defined, the issue requires further study. The use of APAA with directional radiation makes it possible to reduce the average intensity of the created EMB by almost 2 orders of magnitude, making it potentially dangerous only with an average area traffic capacity reaching the upper limit for 5G 10^7 bit/s/m^2. However, it should be taken into account that the use of APAA as BS antenna systems is accompanied by an increase of 1-2 orders of magnitude in their EIRP in main lobe of BS radiation, which significantly increases the spatial separation requirements between APAA and railway equipment falling into the main lobe of APAA radiation.

Discussion

An analysis of the calculated values of the required separation of MC BS and considered railway equipment, which ensures compliance with the requirements of [6-8], indicates the following:

1. I 4G/5G frequency bands of the range 0.8-1 GHz (GSM-900, E-GSM, NR bands 81-83; E_{MPL} = 20 V/m) used mostly for long-distance narrowband low-rate MC services, EIRP value in the main lobe of BS typically does not exceed a few kW and the separation required does not exceed the height of the BS antenna.

2. I 4G/5G frequency bands of the range 1.4-2.7 GHz (GSM-1800, UMTS, LTE, NR bands 1-3, 7, 25, 34, 38, 39-41, 50, 65, 74-76, 84, 86; E_{MPL} = 5–10 V/m), EIRP values in the main lobe of BS can reach 10-20 kW, the necessary spatial separation of railway equipment and BS can reach 100-150 m, but there are no requirements for its mandatory compliance.

3. M frequency bands in the range of 2.7-6.0 GHz (NR bands 1-3, 7, 25, 34, 38, 39-41, 50, 65, 74-78, 84, 86) are increasingly used by 5G systems, including systems which use BS with APAA capable to reach up to 50-100 kW of main-lobe EIRP in the "Beamforming" mode [11, 14], and, at the same time, the susceptibility of the considered railway equipment to EMF exposure in this range is maximum (E_{MPL} = 3 V/m). The necessary spatial separation of BS with this equipment can reach up to half a kilometer, but there are no any requirements for its observance.

4. Fo the railway equipment of the element control level (for example, axle count controllers, controllers for outdoor devices – traffic lights, arrows, means of controlling the free of the path, crossings, etc.), it is impossible to provide protective space zones free from the presence of radiating UE of MC and ensuring the necessary attenuation of UE EM fields.

In particular, if at E_{MPL} = 20 V/m the required spatial separation of railway equipment of the considered type with UE even at the maximum UE EIRP does not exceed 15-24 cm, and the danger of interference to ground-based railway equipment from the UE of 0.8-1.0 GHz range is practically absent, then at E_{MPL} = 5–10 V/m in the range of 1.4–2.7 GHz, the required separation from the UE increases to 0.5–1.0 m, and at E_{MPL} = 3 V/m in the range of 2.7–6.0 GHz it reaches 1.5 m, which today requires the adoption of special restrictions on the use of UEs of the 1.4-6.0 GHz range near railway equipment complying with the requirements of [7, 8], as well as tightening these requirements for equipment of the 1.4-6.0 GHz range at least to the level of requirements adopted for the 0.8-1.0 GHz range.

5. I the near future, it is planned to use widely frequency bands of the FR2 5G range, however, there are no any requirements for the immunity of railway equipment to radio frequency EMFs of this range. Electromagnetic exposures of this range on railway equipment can be the cause of many unpleasant surprises associated with their free penetration inside equipment enclosures through the shield's inhomogeneities and parasitic capacitances of protective filters. The lack of requirements for EMF MPL in this range for railway equipment may cause unacceptable interference for its operation.

Attention should be paid to the coincidence of the EMF MPL range of 3-20 V/m for railway equipment regulated by [6-8] and the MPL EMF range of 2.5-90 μW/cm^2 (3-18.4 V/m), accepted as hygienic standards of many countries, taking into account the danger of non-thermal effects of radio frequency EMF exposure on the human body [22]. This means, in particular, that numerous publications indicating the potential danger of electromagnetic radiation of 4G/5G MC for the population can be considered as the indirect confirmation of their danger to the operation of the corresponding railway equipment. In general, it is possible to comprehensively analyze and solve EMC problems of 4G/5G MC both with equipment of all elements of the infrastructure of a human society and with the population that forms this society.

6. Th above hygienic standards (EMF MPL for population) are limiting average EMF levels affecting the human body, and failures of electronic equipment in many cases are determined by their peak values (pulse amplitudes). In these cases, under pulsed operating modes of MC equipment (TDD modes) and with signal fluctuations in MC radio channels, these peak emissions are 1–2 orders of magnitude higher than the average EMF levels. This circumstance, as well as, in general, a significant complication of the spectral-temporal structure of the MC signals of new generations, can represent an additional danger. For pulsed RF EMFs of other systems, in particular radars, the hygienic MPLs, recalculated to determine the average values (averaging over the period of circular surveillance), are usually 20-100 times lower than for quasi-continuous MC EMFs [23]. With the expected extension of these standards to pulsed EMFs of MC in the future, their requirements will be close to the lowest MPL values for railway equipment adopted in [7, 8].

Considering the relatively low EMF MPL values for the considered railway equipment in UHF and lower part of SHF ranges, it should be recognized that it is relevant to analyze its susceptibility to the exposure of ultra wideband electromagnetic pulses and its protection against such intentional impacts, including tightening the requirements of the relevant standards, since compact generators of such exposures (capable of generating pulses with an amplitude of 10-50 kV/m at a distance of 1-2 m from this sources [24-26]) are capable potentially to disrupt the operation of the considered railway equipment from a distance of hundreds of meters.

7. D endencies in Figure 1-3 indicate that EMB created by radiations of 4G/5G equipment in places with high activity and area density of the population, the wireless information servicing of which by MC systems provides high levels of average area traffic

capacity (up to $10^5 – 10^7$ bit/s/m^2), represents a significant danger to the considered railway equipment.

The average EMB levels, determined by the average levels of EMLA (4), can be significantly reduced by taking measures of a system nature, in particular, by the reduction up to the complete elimination of the influence of intra-network interference (due to the use TDD modes and APAA in beamforming mode with high gains in narrow beams, as well as a significant increase in the amount of radio frequency resource used by MC systems); by the development of infrastructure of MC networks (increase in BS spatial density with a decrease in the communication ranges, rejection of the cellular network structure in favor of an adaptive network structure with the spatial distribution of access points, the use of reconfigurable and absorbing intelligent surfaces, etc.) with a corresponding reduction in the risk of interference to railway signaling and telecommunication equipment, and the corresponding forced risks to public health.

These measures have relatively little effect on the EIRP of BS and UE and on the necessary spatial separation of the MC radiating equipment and the considered railway equipment (calculated values of which are given in Tables 2, 3), and in some cases even increase it (in particular, at a significant increase of EIRP in the main lobe of APAA in Beamforming mode).

Conclusion

The above results indicate a serious potential danger of interference to railway signaling and telecommunication equipment in a complex EME created by a multitude of radiations of 4G/5G MC equipment during the full-scale development and implementation of 4G/5G systems and services. This danger is caused by a huge increase (by several orders of magnitude) in the spatial density of radiation sources, in area traffic capacity and data transmission rates of MC radio channels, provided by high EIRP values of the BS APAA in directions to the served UE.

These results, as well as data [3-5], indicate that the rapid MC evolution 4G□5G□6G, accompanied by a significant complication of EME, violates the previously established balance between the degree of EME complexity and the degree of electromagnetic protection of all types of the infrastructure of modern society. They are intensively saturating with a variety of radio-electronic equipment of limited immunity from unintended and intentional electromagnetic exposures. And since the electromagnetic protection of railway equipment has traditionally been given quite serious attention, it should be expected that technical systems of other types of infrastructure are affected by MC radiations no less than the equipment of railway transport and medical institutions. In this regard, the following should be recognized as relevant:

a) realization of all possible ways to exclude risks of complex EME affect created by 4G/5G systems on the operation of railway signaling and telecommunication equipment. These ways are associated with the tightening of the current standard limits for the immunity of this railway equipment to electromagnetic field in 4G/5G frequency bands, with the limitation of radiation power of 4G/5G base stations located near railway infrastructure facilities, with introducing the requirement of spatial separation between the 4G/5G base stations and the railway infrastructure facilities, and with the imposition of restrictions on the use of 5G mobile stations near railway signaling and telecommunication equipment;

b) performing a similar system EMC analysis for the 4G/5G/6G MC infrastructure and other types of infrastructure of society – economy, defense, public, market, etc., as well as other elements of social and transport infrastructures (in particular, taking into account the development of unmanned vehicles of all types), which allows specifying EMC problems for each of types of infrastructure;

c) substantiation and adoption of adequate requirements of standards for the susceptibility and EMC characteristics of equipment of various types and purposes in all MC frequency bands (in the UHF, SHF & EHF ranges), as well as effective technical, system and managerial measures to ensure the EMC of this equipment, which must be accepted to ensure its reliable functioning in technical systems of all types and elements of public infrastructure during the full-scale implementation of MC 4G/5G/6G systems and services;

d) before the completion of work on items a, b, acceptance, if necessary, of temporary restrictions on the conditions for the joint operation of the 4G/5G MC equipment and critical equipment of other infrastructures – transport, healthcare, economics, etc., ensuring the

protection of equipment and systems of these infrastructures from the impact of MC EMFs (in particular, similar to restrictions adopted to protect the population from MC EMFs, taking into account the closeness of the MPL values of radiofrequency EMFs for technical equipment and for the population).

REFERENCES

[1] IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond, Rec. ITU-R M.2083.
[2] Z. Zhang et.al., “6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies,” *IEEE VT Magazine*, 2019, no. 14 (3), pp. 28-41.
[3] A. Svistunou et.al., “Analysis of EMC between Medical Short-Range Devices and Equipment of Wireless Systems,” *Proc. of the 2021 Joint IEEE Virtual Int. Symp. "EMC-SIPI and EMC Europe"*, July 26 - Aug. 20, 2021, pp. 214-219.
[4] A. Svistunou et.al., “Impact of Electromagnetic Radiation of 4G/5G Base Stations on Medical Short-Range Devices in Urban Area,” *Proc. of the Int. Symp. “EMC Europe 2022”*, Gothenburg, Sweden, Sept. 5-8, 2022, pp. 537-542.
[5] A. Svistunou et.al., “Analysis of EMC between Equipment of Wireless Systems and Medical NB IoT Devices,” *Proc. of the Int. Symp. “EMC Europe 2023”*, Krakow, Poland, Sept. 4-8, 2023, 6 p.
[6] IEC 62236-4:2018. Railway applications - Electromagnetic compatibility – Part 4: Emission and immunity of the signaling and telecommunications apparatus.
[7] UNE EN50121-4: Railway applications. Electro-magnetic compatibility Part 4: Issuance and immunity of signaling and telecommunication devices.
[8] Brodersen RTU32. Test Report. No. 20194-1-R00, 2020. https://cdn.brodersen.com/wp-content/uploads/EN-50121-4-2016-A1-2019.pdf.
[9] ETSI TS 136 104 V15.8.0 (2019-10). LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception (3GPP TS 36.104, vers. 15.8.0 Rel. 15).
[10] ETSI EN 301908-24. IMT cellular networks; Harmonized Standard for access to radio spectrum; Part 24: New Radio (NR) Base Stations (BS); Rel. 15.
[11] H. Aspund et al., “Advanced Antenna Systems for 5G Network Deployments. Bridging the Gap Between Theory and Practice,” Academic Press, 2020, 713 p.
[12] ETSI TR 136 942 V17.0.0 (2022-04). LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Frequency (RF) system scenarios.
[13] AAU5613 Product Description. Huawei Technologies Co., Ltd., 2018, 18 p.
[14] Nokia Solutions and Networks AirScale MAA 64T64R 128AE B41 120W AAHF AAHF-01. https://fccid.io/VBNAAHF-01
[15] ETSI TS 136 101 V15.10.0 (2020-04). LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception (3GPP TS 36.101, vers. 15.10.0 Rel. 15).
[16] ETSI EN 301 908-25. IMT cellular networks; Harmonised Standard for access to radio spectrum; Part 25: New Radio (NR) User Equipment (UE).
[17] V. Mordachev, “Estimation of Electromagnetic Background Intensity Created by Wireless Systems in Terms of the Prediction of Area Traffic Capacity,” *Proc. of the Int. Symp. "EMC Europe 2019",* Barcelona, Spain, Sept. 2-6, 2019, pp. 82-87.
[18] V. Mordachev, “Electromagnetic Background Generated by Mobile (Cellular) Communications,” *Proc. of the Asia Pacific Int. Symp. on EMC (Hybrid Conf.) APEMC 2021*, Bali-Indonesia, Sept. 27-30, 2021, pp. 37-40.
[19] V. Tikhvinskiy, S. Terentiev and V. Visochin, “LTE/LTE Advanced Mobile Networks: 4G technologies, applications architecture,” Moscow: Media Publisher, 2014. 384 p.
[20] Guidelines for evaluation of radio interface technologies for IMT-2020. Report ITU-R M.2412.
[21] International Commission on Non-Ionizing Radiation Protection (ICNIRP). Guidelines for limiting exposure to electromagnetic Fields (100 kHz to 300 GHz). Health Physics. 2020, no. 118(5), pp. 483-524.
[22] V. Mordachev, “Refined Analysis of the Correlation Between the Accepted Maximum Permissible Levels of Radio Frequency Electromagnetic Fields for the Population and the Lethality Rate of Covid-19,” *Doklady BGUIR*. 2022, no. 20(1), pp. 55-64. http://dx.doi.org/10.35596/1729-7648-2022-20-1-55-64.
[23] O. Grigoriev, Y. Zubarev, “The effects of wireless communication electromagnetic energy influence on persons: predictions of the growth for conditioned morbidity, their implementation and problems of evaluation,” *CONCEPCII.* 2022, no. 41(1), pp. 3-17.
[24] IEC TR 61000-4-35. Electromagnetic compatibility (EMC) – Part 4-35: Testing and measurement techniques – HPEM simulator compendium, Geneva, Switzerland, 2009.
[25] A.S. Pastukh, V.O. Tikhvinskiy, E.E. Devyatkin, A.A. Savochkin, A.V. Lukyanchikov “Electromagnetic compatibility studies between HAPS and IMT terrestrial networks of legacy mobile standards (GSM, UMTS, LTE) in the frequency bands below 2.7 GHz,” *T-Com*m, 2024, vol. 18, no.5, pp. 49-60. doi: 10.36724/2072-8735-2024-18-5-49-60.
[26] V.O. Tikhvinsky, "International regional problems of electromagnetic compatibility: results of the symposium EMC Europe-24," *T-Comm*, 2024, vol. 18, no. 9, pp. 36-40. doi: 10.36724/2072-8735-2024-18-9-36-40.

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

RFID TECHNOLOGIES: ANALYSIS OF CURRENT STATUS AND DEVELOPMENT

Artem Dymkov [1, 2]

[1] Institute of Radio and Information Systems (IRIS), Vienna, Austria;

[2] MIREA – Russian Technological University, Moscow, Russia

dymkov@media-publisher.eu

ABSTRACT

Radio communication is a convenient and very common way of organizing wireless transmission of information. It has a long history. In addition to the usual over-the-air television and radio broadcasting, today there are a large number of different technologies with their own characteristics. However, the development of science, as well as the constantly growing demands and needs of a person suggest the emergence of problems, the solution of which leads to the development of new technologies and devices that provide reliable and stable communication in many industries. RFID (Radio Frequency IDentification) technology is one of the most frequently used technologies in the modern world. It uses an automatic data collection system that helps to improve the efficiency of the system. The article analyzes RFID technologies and the possibilities of their application. The purpose of the scientific research is to analyze the main functions of radio frequency identification technology, examples of the implementation and use of this technology are given, the main advantages and disadvantages are described. An assessment is given of the prospects for the introduction of RFID tags in various sectors of the economy. The relevance of the study of the current state is presented and the prospects for the development of these technologies are analyzed.

KEYWORDS: *Radio Frequency IDentification, RFID tags classification*

DOI: 10.36724/2664-066X-2024-10-5-33-41

Received: 20.09.2024
Accepted: 17.10.2024

Citation: Artem Dymkov, "RFID technologies: analysis of current status and development" *Synchroinfo Journal* **2024**, vol. 10, no. 5, pp. 33-41

Licensee IRIS, Vienna, Austria.

Introduction

RFID (Radio Frequency IDentification) technology is one of the most widely used technologies in the modern world. RFID technology uses an automatic data collection system that helps improve the efficiency of the system. A combination of a tag and a reader is used for identification. The code is stored in the RFID tag, and this tag is attached to a physical object, making the object unique and identifiable. The object then transmits the code from the tag. Thus, the reader receives information about the object.

RFID technology, in the sense in which we understand it today, appeared in the 1980s, although the history of radio frequency identification takes us back to an earlier period - to the end of the 19th century, when the British physicist James Clerk Maxwell formulated the theory of a unified electromagnetic field. A huge role in the development of the technology was played by the Second World War, when it became necessary to find a reliable way to identify aircraft: whether they belong to friendly aviation or to the enemy. Modern RFID systems are based on the same principles: they either “wake up” by reflecting a signal, as in the case of passive tags (RFID), or they themselves transmit a signal if active tags are used (Real-Time Locating Systems, RTLS). The evolution of RFID technology has led to the spread of solutions for identification (passive identification technologies) and solutions for real-time monitoring (active identification technologies).

Current state and development of RFID technology

RFID (Radio Frequency IDentification) is a method of automatic identification of objects, in which data stored in so-called transponders, or RFID tags, is read or written using radio signals.

This is a rapidly developing technology that offers many advantages over traditional identification devices, such as barcodes, as it can read data from a tag without direct line of sight. This technology is more effective when a longer reading range, fast scanning, and flexible data transfer capabilities are required [1].

Any RFID system consists of a reading device (reader, interrogator) and a transponder (also known as an RFID tag, sometimes also called an RFID tag).

By reading range, RFID systems can be divided into systems:

• s ort-range identification (reading at a distance of up to 20 cm);
• medi m-range identification (from 20 cm to 5 m);
• lon -range identification (from 5 m to 300 m).

Most RFID tags consist of two parts. The first is an integrated circuit (IC) for storing and processing information, modulating and demodulating a radio frequency (RF) signal and some other functions. The second is an antenna for receiving and transmitting a signal.

Already known RFID applications (contactless cards in access control and management systems, long-range identification systems and payment systems) are gaining additional popularity with the development of Internet services.

There are several ways to systematize RFID tags and their systems:

• By op rating frequency
• Ta s of the LF (125-134 kHz); HF (13.56 MHz); UHF (860-960 MHz)
• Near-field UHF adio frequency tags
• By power source
• Passive
• Active
• Semi-passive
• By me ory type
• RO (Read Only)
• W RM (Write Once Read Many)
• RW (Read nd Write)
• By execution

RFID devices provide unique identification of objects scanned by a reader to obtain information recognizing a specific object, such as a serial number. The chip on an RFID device is capable of transmitting up to 2000 bytes of data.

Figure 1 shows the operation diagram of this technology.

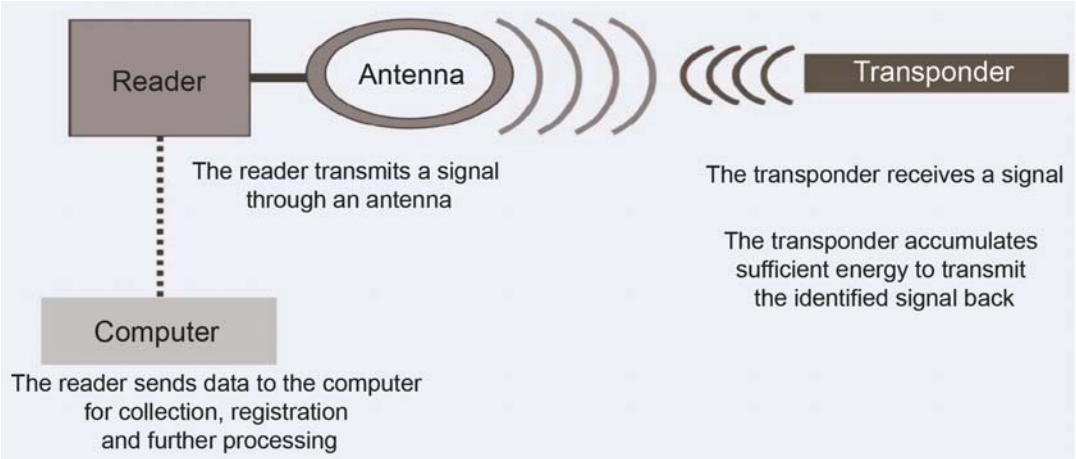


Fig. 1. RFID technology operation diagram

As an example, we can cite the structural diagram of rewritable LF range RFID microcircuit from Microchip ATA5577C (Fig. 2).

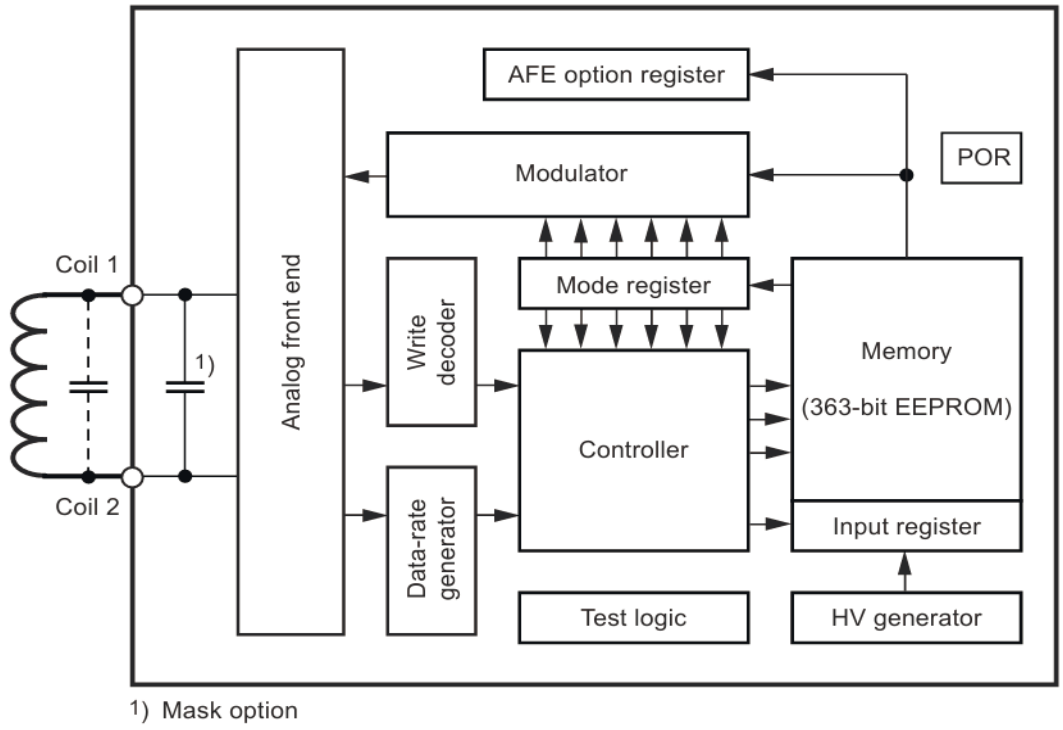


Fig. 2. Structural diagram of the ATA5577C chip

An example of its operation protocol is shown in Figure 3. Technical data for the ATA5577C microcircuit from Microchip are available at https://ww1.microchip.com/downloads/aemDocuments/documents/WSG/ProductDocuments/DataSheets/ATA5577C-Read-Write-LF-RFID-IDIC-100-to-150-kHz-Data-Sheet-DS70005357B.pdf.

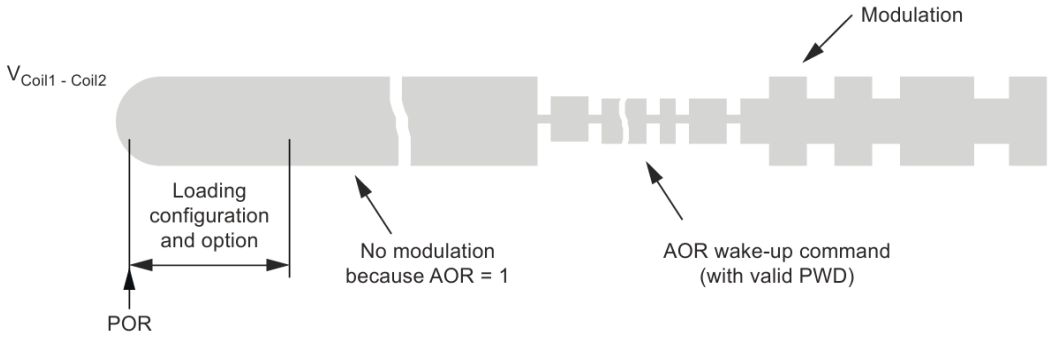


Fig. 3. Example of operation of the ATA5577C chip

Some innovative RFID solutions include:
– RFID deployment kits used in the military at remote stations to track incoming items;
– RFID tag for government postal services to efficiently track and deliver packages;
– RFID smart chips improve recognition and security at international airports;
– ease of hotel and motel booking and visits, billing and payment in stores.
Some of the most significant benefits of implementing RFID technology include:
– efficient informati n processing;
– red ction of excess inventory and in out-of-stock situations;
– high-quali y and fast customer service;
– impr ved forecasting and planning.

RFID technology in the UHF range has become actively used around the world as a tool for mass identification of objects outside the direct line of sight of reading devices at distances of up to 10 m with identification speeds of up to 1000 unique objects per second [8-10]. Frequently used technologies for recognizing objects, goods, materials, along with RFID tags, are QR codes and barcoding.

Based on the data in Table 1, you can see both the advantages and disadvantages of this technology. The advantages of RFID compared to its analogues are: the ability to rewrite – this reduces the cost of purchasing a new RFID tag, there is no need for direct visibility – you can place such tags covertly, a large reading distance and data storage capacity, support for reading multiple tags, resistance to environmental influences, a high degree of security – the inability to change the identifier number that is assigned to the tag during the production process, which guarantees a high degree of protection against counterfeiting.

Table 1

Comparison of RFID technologies with barcode and QR code

Technology characteristics	**RFID**	**Barcode**	**QR-код**
Need for direct visibility of the tag	Possible reading of hidden tags	Reading with line of sight only	Reading with line of sight only
Memory capacity	from 10 to 512 000 bytes	up to 100 bytes	No
Ability to rewrite data and reuse the tag	Exists	No	No
Registration range	to 100 m	to 4 m	to 1 m
Simultaneous identification of several objects	to 200 tags/second	Impossible	Depends on the reader
Resistance to environmental influences	Increased strength and resistance	Depends on the material it is applied to	Depends on the material it is applied to
Service life	More than 10 years	Depends on the printing method and the material it is applied to	Depends on the printing method and the material it is applied to
Security and protection against counterfeiting	Can't be faked	Easy to fake	Easy to fake
Use of both stationary and hand-held terminals for identification	Yes	Yes	Yes
Price	High	Low	Low

Security is also guaranteed by the fact that the RFID tag can password-protect the data recording and reading operations, as well as encrypt their transmission. One tag can simultaneously store open and closed data.

However, this system also has its drawbacks: the cost of implementing RFID tags is higher than that of a barcode and QR code, there is a difficulty in self-production, and there is also susceptibility to interference in the form of electromagnetic fields.

Speaking of international standards, RFID technologies, as an integral part of automatic identification, are developed and adopted by the international organization ISO together with IEC.

The cost of RFID tags is decreasing by 5-10% every year. Obviously, there is a limit to this reduction, since it will always be more expensive to create a tag than a barcode or QR code, its cost is made up of the price of the electronic device, chip, antenna, multilayer structure.

RFID applications use several frequencies: 123 kHz, 13.57 MHz and 850-940 MHz for passive RFID; 423 MHz and 2.55 GHz for active RFID. Global standardization of RFID systems is a serious issue.

Below is a short list of RFID standards: ISO 1024, ISO 1036, ISO 1194, ISO 1443, ISO 1593, IS0 1800, EPC global. These standards govern the communication between the RFID reader and the tag. Standards operate in selected frequency ranges, such as 863-926 MHz for UHF or 13.66 MHz for HF).

The combination of RFID technology and computing technology is called an "RFID system" and consists of the following components:

• Tag/tr nsponder (electronic label);

• Antenna (tag reading medium);

• R ader/interrogator (reads tag information);

• Communication infrastructure (allows the reader/RFID to operate through the IT infrastructure);

• Application software (user database / application / interface).

An RFID tag is a small electronic device, also called a transponder. The tag consists of a simple silicon microchip and an antenna. The tag can be attached to an object, usually an item, a box. The information is collected by the chip and can be transmitted wirelessly. An RFID tag can be active (with batteries), passive (without batteries) and semi-passive (hybrid). The tag has an identification code that can be transmitted to the reader.

RFID antennas are used to collect information about any item. There are many types of RFID antennas such as patch antennas, linearly polarized antennas, whip antennas and adaptive antennas, gate antennas and omnidirectional antennas.

An antenna designer first creates a known antenna and then modifies its physical parameters to obtain an optimal bandwidth. In the past few years, researchers have studied the design of circularly polarized antennas. A dual-polarized antenna can be used. This antenna is suitable for passive operation at 5.4 GHz in RFID applications. Microstrip antennas are used for RFID, which have attractive features such as light weight, small volume, low profile and low manufacturing cost.

RFID is a modern technology that has changed the methods of identifying and tracking objects [2-7]. The areas of application of RFID technology are shown in Table 2.

Table 2

Applications of RFID technology

Areas of application	Application
Warehouse logistics	Allows you to: track goods in the warehouse in real time, which ensures accurate inventory and control; ensure the movement of products to optimize processes; minimize personnel errors when forming orders; reduce operating costs, thanks to automation.
Retail	RFID tags continuously collect information about the location of goods from the distribution center to the retail point of sale for inventory management. Collecting data on customer preferences and purchase history to provide personalized offers and promotions. Implementing self-service checkouts with RFID readers for faster and more convenient payment for purchases.
Manufacturing sector	Accurately track inventory levels to optimize the supply chain and prevent production disruptions. Track the location and condition of production assets (tools, equipment, vehicles) to improve service efficiency and prevent losses.
Food industry	Inventory management, tracking food products throughout the supply chain to ensure consumer safety and regulatory compliance. Using RFID tags with temperature sensors to monitor and maintain food storage and transportation conditions.
Agriculture	Livestock tracking, crop management to optimize resource use, automation of animal feeding and harvesting processes.
Healthcare	Tracking stock levels of medicines and medical supplies to prevent shortages and optimize procurement. Identifying patients, monitoring their movements and ensuring their safety in healthcare facilities, using sensors to monitor patients' vital signs.

The main advantages of using RFID technology:

– Each RFID tag has a built-in unique code that distinguishes it from all the others;

– RF D allows data to be read and written from multiple tags simultaneously, making it more efficient to track large inventories;

– RFID tags can be read without being in line of sight, which allows you to track items in hard-to-reach places;

– Data on RFID tags can be rewritten, allowing information about items to be updated as they move;

– RFID systems can automate the inventory process, saving time and resources;

– RFID uses wireless communication, allowing items to be tracked without the need for a physical connection;

– RFID provides continuous tracking of the item location, allowing operators to track them in real time;

– RFID can automate product inspection on assembly lines, increasing efficiency and reducing the likelihood of errors;

– RFID technology can improve the accuracy and speed of order picking, ensuring that customers receive the correct items.

The main obstacles to the spread of RFID technology are:

– RFID tags can be relatively expensive, limiting their use for tracking low-cost items;

– RFID systems can be sensitive to external factors such as humidity and metal surfaces, which can affect their effectiveness;

– The lack of uniform industry standards for RFID systems can make them difficult to integrate with different technology systems;

– RFID tags can be vulnerable to unauthorized reading and cloning, which compromises data security.

These limitations are gradually being eliminated as the technology advances. The cost of RFID tags is decreasing. RFID systems are being developed to be more resistant to factors such as humidity and metal surfaces. Efforts are underway to develop and

implement industry standards for RFID systems, making it easier to integrate them with other technologies. Research and development is aimed at improving the security of RFID systems, including encryption and authentication methods to protect data from unauthorized access. The future of RFID technology looks quite promising, despite some problems that have not yet been resolved, in particular, the shortage of chips and other raw materials. Forecasting shows that the global RFID market will continue to expand. Thus, by 2030, the RFID tag market is predicted to reach $ 54.7 billion with a CAGR of 15.9%. The world is currently seeing the rapid development of chipless RFID tag technology, with the market valued at $0.89 billion in 2019 and expected to reach $3.94 billion by 2025, with a CAGR of 28% over the forecast period 2020-2025.

RFID tags classification by power source, memory type and operating frequency

Classification of RFID tags by power source

RFID tags, depending on the presence or absence of a power source, can be classified as passive, active and semi-passive [6]. Let's consider their features and areas of application.

Passive RFID tags

Passive RFID tags do not have a built-in power source. The electric current induced in the antenna by the electromagnetic signal from the reader provides sufficient power for the operation of the silicon CMOS chip located in the tag and the transmission of a response signal. Commercial implementations of low-frequency RFID tags can be built into a sticker or implanted under the skin.

The compactness of RFID tags depends on the size of the external antennas, which are many times larger than the chip and, as a rule, determine the dimensions of the tags. Due to the range of antenna sizes, tags have different sizes - from a postage stamp to a postcard. In practice, the maximum reading distance of passive tags varies from 10 cm (4 inches) (according to ISO 14443) to several meters (EPC and ISO 18000-6), depending on the selected frequency and the size of the antenna. In some cases, the antenna can be made using a printed method.

Non-silicon tags can be made of polymer semiconductors. Currently, several companies around the world are developing them.

Passive tags of the UHF and microwave ranges (860-960 MHz and 2.4-2.5 GHz) transmit a signal by modulating the reflected signal of the carrier frequency (Backscattering Modulation). The reader antenna emits a signal of the carrier frequency and receives the modulated signal reflected from the tag. Passive tags of the HF range transmit a signal by modulating the load of the carrier frequency signal (Load Modulation). Each tag has an identification number. Passive tags can contain rewritable non-volatile memory of the EEPROM type. The range of the tags is 1-200 cm (HF tags) and 1-10 m (UHF and microwave tags).

Active RFID tags

Active RFID tags have their own power source and do not depend on the energy of the reader, as a result of which they are read at a long distance, are larger in size and can be equipped with additional electronics. However, such tags are the most expensive, and the batteries have a limited operating time. Active tags are in most cases more reliable and provide the highest reading accuracy at a maximum distance. Having their own power source, they can also generate an output signal of a higher level than passive ones, allowing them to be used in environments that are more aggressive for radio frequency signals: water (including people and animals, which mainly consist of water), metals (ship containers, cars), for long distances in the air.

Most active tags can transmit a signal over distances of hundreds of meters with a battery life of up to 10 years. Some RFID tags have built-in sensors, for example, for monitoring the temperature of perishable goods. Other types of sensors in combination with active tags can be used to measure humidity, shock/vibration, light, radiation, temperature, and atmospheric gases (such as ethylene). Active tags typically have a much larger reading range (up to 300 m) and memory capacity than passive tags, and are capable of storing more information for transmission by the transceiver.

Semi-passive RFID tags

Semi-passive RFID tags, also called semi-active, are very similar to passive tags, but are equipped with a battery that supplies the chip with energy. The range of these tags depends only on the sensitivity of the receiver - reader and they can function at a greater distance and with better characteristics.

Classification of RFID tags by memory type

RFID tags can be classified by the types of memory used as follows:

• RO (Read Only) - data is written only once, immediately upon manufacture. Such tags are suitable only for identification. No new information can be written to them, and they are almost impossible to counterfeit.

• WORM (Write Once Read Many) - in addition to a unique identifier, such tags contain a block of write-once memory, which can then be read many times.

• RW (Read and Write) - such tags contain an identifier and a memory block for reading / writing information. The data in them can be rewritten many times.

Classification of RFID tags by operating frequency

RFID tags operate in frequency ranges from hundreds of kilohertz to hundreds of megahertz. The radio frequencies used largely determine their functional parameters and are discussed in more detail below.

LF range tags (125-134 kHz)

Passive systems in this range have low prices and, due to their physical characteristics, are used for subcutaneous tags when chipping animals and people. However, due to the wavelength, there are difficulties with reading over long distances.

HF range tags (13.56 MHz)

13 MHz range systems are inexpensive, have no environmental or licensing issues, are well standardized, and have a wide range of solutions. They are used in payment systems, logistics, and personal identification. The ISO 14443 standard (types A/B) has been developed for the 13.56 MHz frequency. Unlike Mifare 1K, this standard provides a key diversification system, which allows creating open systems. Standardized encryption algorithms are used. Several dozen systems have been developed based on the ISO 14443 B standard, for example, the Paris region public transport fare payment system. Serious security problems were found for the standards that existed in this frequency range: the cheap Mifare Ultralight card chips, introduced in the Netherlands for the OV-chipkaart urban public transport fare payment system, had no cryptography at all; later, the Mifare Classic card, which was considered more reliable, was hacked.

As with the LF range, systems built in the HF range have problems with reading from long distances, reading in high humidity conditions, the presence of metal, as well as problems associated with the occurrence of collisions during reading.

UHF range tags (860-960 MHz)

Tags in this range have the longest detection range, and many standards in this range have anti-collision mechanisms. For a long time, there were no chips that would fully meet these requirements. Currently, the UHF frequency range is open for free use in the Russian Federation in the so-called "European" range – 863-868 MHz.

Near-field UHF radio frequency tags

Near-field tags, not being directly radio tags, but using the antenna's magnetic field, allow solving the problem of reading in conditions of high humidity, the presence of water and metal. With the help of this technology, RFID tags began to be used in the retail trade of pharmaceutical products (requiring authenticity control, accounting, but often containing water and metal parts in the packaging).

Conclusion

The article analyzes the advantages and limitations of using RFID technology, classifies RFID tags. It also compares radio frequency identification technology with bar coding and QR coding technology. The current state and development prospects of RFID technology are analyzed also. To summarize, it can be said that digitalization is really actively penetrating all sectors of the economy. RFID technology is one of many examples. It is possible to highlight the changes associated with digitalization that are currently taking place in industry. Despite the high cost, experts are optimistic about the future prospects for the implementation of radio frequency identification technology, believing that it will subsequently replace bar coding, affect all business processes and change wholesale and retail trade.

REFERENCES

[1] A.O. Fomchenkov, A.A. Kiktev, "Radio frequency identification technology," *Advanced materials and technologies (PMT-2022): Collection of reports of the conference of the Institute of Advanced Technologies and Industrial Programming of the Russian Technological University MIREA*, Moscow, April 11-15, 2022 / Ed. A. N. Yurasov. Vol. 1. Moscow: MIREA – Russian Technological University, 2022, pp. 529-532.

[2] M.M. Kulikov, M.A. Komissarova, I.A. Nazarova, "Prospects for the use of RFID technologies in Russia," *Bulletin of the Rostov State University of Economics*. 2022. No. 4 (80). Pp. 190-197. DOI 10.54220/v.rsue.1991-0533.2023.80.4.026.

[3] A. Subrahmannian and S. K. Behera, "Chipless RFID Sensors for IoT-Based Healthcare Applications: A Review of State of the Art," in IEEE Transactions on Instrumentation and Measurement, vol. 71, pp. 1-20, 2022, Art no. 8003920, doi: 10.1109/TIM.2022.3180422.

[4] S. K. Behera, "Chipless RFID Sensors for Wearable Applications: A Review," *IEEE Sensors Journal*, vol. 22, no. 2, pp. 1105-1120, 15 Jan.15, 2022, doi: 10.1109/JSEN.2021.3126487.

[5] J. Su, Z. Sheng, A. X. Liu, Y. Han and Y. Chen, "Capture-Aware Identification of Mobile RFID Tags with Unreliable Channels," *IEEE Transactions on Mobile Computing*, vol. 21, no. 4, pp. 1182-1195, 1 April 2022, doi: 10.1109/TMC.2020.3024076.

[6] K. Niotaki et al., "RF Energy Harvesting and Wireless Power Transfer for Energy Autonomous Wireless Devices and RFIDs," *IEEE Journal of Microwaves*, vol. 3, no. 2, pp. 763-782, April 2023, doi: 10.1109/JMW.2023.3255581.

[7] J. Xu et al., "The Principle, Methods and Recent Progress in RFID Positioning Techniques: A Review," *IEEE Journal of Radio Frequency Identification*, vol. 7, pp. 50-63, 2023, doi: 10.1109/JRFID.2022.3233855.

[8] T.N. Yelina, S.V. Bezzateev, S.G. Fomicheva, "The use of passive radio frequency tags in decentralized information exchange systems," *T-Comm*, 2023. vol. 17, no.9, pp. 38-47. DOI: 10.36724/2072-8735-2023-17-9-38-47.

[9] R. Chen, X. Huang, Y. Zhou, Y. Hui and N. Cheng, "UHF-RFID-Based Real-Time Vehicle Localization in GPS-Less Environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 9286-9293, July 2022, doi: 10.1109/TITS.2021.3085824.

[10] A. Motroni, F. Bernardini, A. Buffi, P. Nepa and B. Tellini, "A UHF-RFID Multi-Antenna Sensor Fusion Enables Item and Robot Localization," *IEEE Journal of Radio Frequency Identification*, vol. 6, pp. 456-466, 2022, doi: 10.1109/JRFID.2022.3166354.

SYNCHROINFO JOURNAL

EMC EUROPE-24: INTERNATIONAL PROBLEMS OF ELECTROMAGNETIC COMPATIBILITY:

Valery Tikhvinskiy [1, 2]

[1] Institute of Radio and Information Systems (IRIS), Vienna, Austria;

[2] International Information Technologies University (IITU), Almaty 050000, Kazakhstan

vtniir@mail.ru

ABSTRACT

The article reviews the latest scientific achievements in the field of electromagnetic compatibility, presented at the international regional symposium on electromagnetic compatibility "EMC Europe 24" by the leading EMC research organizations, European, Asian, African and South American universities, as well as the largest companies, microelectronics manufacturers, automotive and aviation companies. The symposium "EMC Europe" is the leading international regional symposium on electromagnetic compatibility and continues a long tradition of regular international symposiums on EMC, organized in Europe. The symposium considered the following issues: EMC of 5G, 6G networks and the Internet of Things (IoT); standards and regulations, EMC management, EMC education; risk-based EMC, electromagnetic immunity; EMC in safety and security applications, in industrial environments and in military applications; Electromagnetic environment, lightning protection, intentional EMF and EMP, high-power electromagnetic interference, electrostatic discharges; wired and wireless communications, UWB, power line communications, spectrum management; automotive, rail, naval, aviation and space systems. The article presents the results of studies on the assessment of the EMC impact of Wi-Fi device transmitters (RLAN networks) on 5G radio receivers, the application of models developed for assessing the shielding properties of a wide range of products made of composite materials, the study of the characteristics and development of nonlinearity models of radio frequency amplifiers (RFAs) of the FR1 range of 5G networks for their subsequent application in solving EMC problems of radio equipment for mobile (cellular) communications in complex EMC created in the 4G/5G frequency bands, etc.

KEYWORDS: *electromagnetic compatibility, EMC Europe-24, frequency range, 5G networks*

DOI: 10.36724/2664-066X-2024-10-5-42-46

Received: 15.09.2024
Accepted: 10.10.2024

Citation: Valery Tikhvinskiy, "EMC Europe-24: International Problems of Electromagnetic Compatibility" *Synchroinfo Journal* **2024**, vol. 10, no. 5, pp. 42-46

Introduction

From September 2 to 5, 2024, the second significant international regional symposium on electromagnetic compatibility "EMC Europe-24" was held in Bruges (western Belgium) at the VMCC Congress and Assembly Center, the other - the Asia-Pacific symposium AREMS-24 was held at the end of May 2024 in Naha on Okinawa Island (Japan). The symposium "EMC Europe-24" brought together more than 700 participants from more than 50 countries, representing leading EMC research organizations, European, Asian, African and South American universities, as well as major companies, microelectronics manufacturers, automotive and aviation companies.

The EMC Europe Symposium is the leading international regional symposium on electromagnetic compatibility and continues a long tradition of regular international EMC symposia organised in Europe: at the Wroclaw University of Technology since 1972 (20 annual symposia) and at the Zurich University of Technology (also 20 annual symposia since 1973), as well as other European symposia that were organised in Rome (since 1994) and later in Bruges, Sorrento, Eindhoven, Barcelona and Hamburg. Each of these three EMC symposia was held every two years. Since 2010, these scientific forums have been united into EMC Europe – the International Symposium and Exhibition on Electromagnetic Compatibility.

EMC Europe is now organized annually in a European city with an EMC research center to provide an international forum for leading scientists and experts to exchange technical information on EMC. Joint EMC Europe symposia have been organized in Wroclaw (2010, 2016), York (2011), Rome (2012, 2020), Bruges (2013), Gothenburg (2014, 2022), Dresden (2015), Angers (2017), Amsterdam (2018), Barcelona (2019) and Glasgow (2021 – virtual) – these symposia have become joint symposia of the IEEE International Symposium on EMC and EMC Europe.

The 15 sessions of the EMC Europe 24 Symposium covered the following topics: EMC of 5G, 6G and the Internet of Things (IoT); Standards and Rules, EMC Management, EMC Education; Risk-based EMC, Electromagnetic Immunity; EMC in Safety and Security Applications; EMC in Industrial and Enterprise Environments; EMC in Military Applications; Electromagnetic Environment, Lightning Protection, Intentional EMI/EMF, High Power Interference, Electrostatic Discharge; Wired and Wireless Communications, UWB, Power Line Communications, Spectrum Management; Automotive, Rail, Naval, Aviation and Space Systems.

Electromagnetic compatibility issues

The plenary session of the EMC Europe 24 Symposium featured papers on the electromagnetic compatibility scientific research programmes within the work framework of the European Research Agency (REA) and Phillips on ensuring EMC of medical devices when they are used in modern medicine.

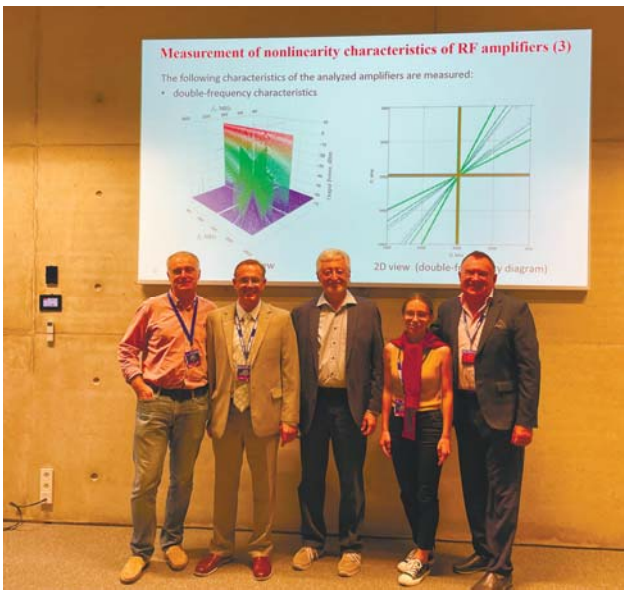
First report by REA specialists presented the possibilities of cooperation between scientists within the framework of international doctoral research programs as a form of combining efforts for scientists and specialists from different countries in solving EMC problems in the form of temporary creative associations with centralized funding at the international level with a total volume of 606 million euros over the next three years.

The main target funding of the program is 417 million euros, which is aimed at financing the research of postgraduate students studying EMC problems at the university level and combining their efforts in a single network structure of researchers of EMC prospects. In addition to the effectiveness of research, the program pays great attention to innovation and patenting of the obtained results. The second report was devoted to EMC management issues based on the functional safety risks in medical devices design. Due to the fact that electromagnetic environments are becoming less predictable, passing EMC tests based on current standards does not mean that the medical device will be safe and effective in the intended environment of use. To reduce the risks of medical devices functional safety, a combination of solving electromagnetic compatibility and functional safety issues during the design is proposed to achieve a comprehensive solution for the safety of medical devices.

Traditionally, for more than 10 years, one of EMC Europe important sections was a session organized by scientists from the EMC Research Laboratory of the Belarusian State University of Informatics and Radioelectronics (NIL EMC BSUIR, https://emc.bsuir.by/), dedicated to comprehensive diagnostics of EMC of complex systems and headed by BSUIR professor V.I. Mordachev.

Several interesting reports were made at the session. For example, the report of professor V.I. Mordachev was devoted to the development of a technology for analyzing the statistical characteristics of the electromagnetic environment (EME) near the earth's surface, created by emissions from mega-constellations of low-orbit communication satellites such as Starlink, OneWeb, etc. [1-8]. Presented a method for predicting the average intensity of the electromagnetic background (EMF) generated by these satellites, based on the statistical theory of EMF developed by the author and linking the average EMF levels with the number of satellites in the group, the parameters of their radiation on the main and side lobes, orbital altitudes and limitations on the elevation angle of ground equipment servicing.

The calculation results showed that the expected EMF levels of the microwave range generated by mega-constellations of low-orbit communication satellites are safe, since they are many orders of magnitude lower than the accepted maximum permissible level of radio frequency EMF for the population, but at the same time they are many orders of magnitude higher than the levels of EMF of natural origin, which significantly changes the physical characteristics of the habitat and requires serious attention and analysis [9-11].



During the session, the Deputy Head of the Research Laboratory of EMC BSUIR Sinkevich E.V. made reports on behalf of the international cooperation of scientists. His first report was devoted to the results of experimental studies of the characteristics and development of nonlinearity models of radio frequency amplifiers of the FR1 range of 5G networks for purpose of their subsequent application in solving problems for radio equipment – mobile (cellular) communications EMC in complex EMO created in the 4G/5G frequency bands [12-17]. The amplifier characteristics were measured using the original dual-frequency probing technology in n7 range (2500-2570 / 2620-2690 MHz), which is allocated in the Republic of Belarus for 4G mobile communication systems, and n78 frequency range (3300-3800 MHz) of 5G mobile communication systems. Based on the results of measuring dual-frequency characteristics of amplifiers, their single-signal amplitude characteristics, as well as dual-signal amplitude characteristics and values of the dynamic range for intermodulation 3rd, 5th, 7th and 9th orders in first harmonic zone, polynomial models of 27^{th}-37th orders were synthesized, adequately describing the studied amplifiers transfer characteristics both in low nonlinearity region and in the saturation region.

The synthesized models cover a wide dynamic range of input effects while simultaneously analyzing nonlinear effects of all types, including intermodulation, blocking and crosstalk. Using the original technology of discrete nonlinear EMC analysis. This technology is invariant to EMO complexity for a polynomial models fixed order of the RF amplifier transfer characteristics, obtained models provide high efficiency of nonlinear processes quantitative analysis and radio interference.

And in arising in 4G/5G equipment and networks for any practically achievable number of input unwanted signals distributed in a dynamic range of up to 200 dB.

An interesting report was presented by E.V. Sinkevich. He considered models developed application for assessing the shielding properties of a wide range for composite materials products made: silicone and rubber conductive gaskets, conductive adhesives and paints, absorber panels. The models allow calculating the shielding efficiency of gaskets and analyzing absorbers based on their geometric parameters and general information about the internal composite material structure.

An analytical model of composite materials conductivity with conductive fillers, based on the percolation theory, has high computational efficiency and is applicable in a wide frequency range. It is used to describe the shielding properties of conductive silicone, rubber, conductive materials based on foamed polyurethane, as well as to assess the reflectivity and shielding properties of absorber panels.

An empirical model for assessing gaskets shielding efficiency made of composite materials is based on representing the gasket as an equivalent wire mesh. This model can be used in designing electromagnetic protection of the system in cases where information on the internal structure of the composite gasket is missing. The developed models validity was confirmed by comparison with experiments results in frequency range from 800 MHz to 16 GHz.

In this session of the EMC Europe-24 symposium, a member of the Synchroinfo Journal editorial board, professor, Doctor of Economics V. O. Tikhvinsky took part with a report from a team of scientists. The results of theoretical studies were presented on assessing the EMC impact of Wi-Fi device transmitters (RLAN networks) on 5G radio receivers (UE subscriber devices and gNB base stations) in the range of 6425-7125 MHz in dense urban areas.

The report noted that at WRC-23 (Dubai, UAE), the frequency bands 6425-7125 MHz in Region 1, in some countries in Region 2 and 7025-7125 MHz in Region 3 were identified for use by Administrations wishing to implement the terrestrial component of International Mobile Telecommunications (IMT), including IMT-2020/5G. Some Administrations plan to simultaneously implement 5G and Wi-Fi networks on common frequency channels, as well as RLANs in this upper half of the 6 GHz frequency range.

Calculations have shown that in dense urban areas in the frequency range 6425-7125 MHz, 5G gNB base station transmitters at ranges greater than 50 m from Wi-Fi located inside buildings do not affect LBT devices designed to prohibit Wi-Fi operation in conditions of unintentional interference in the operating channel. Based on the results of the probabilistic EMC assessment (SEAMCAT 5.5.0) obtained by the authors, the levels of throughput reduction of UE subscriber devices and gNB base stations were estimated under the group impact of 50, 100 and 200 Wi-Fi transmitting devices on them and a conclusion was made about the impossibility of joint operation without frequency spacing, which was reported at the symposium "EMC Europe-24".

Conclusion

The EMC Europe 2024 Symposium aims to be a dynamic platform where leading experts, researchers and practitioners come together to share their latest findings, hold lively discussions and establish collaborations that will drive the field of electromagnetic compatibility forward. With a carefully curated programme including keynote speeches, technical sessions, workshops and tutorials, EMC Europe aim to explore the frontiers of EMC, covering a wide range of topics such as measurement techniques, computational electrodynamics, electromagnetic risk management and more.

The next stage of holding international regional symposia on EMC in 2025 will include holding the symposia AREMS-25 in May on Taiwan Island (China) and "EMC Europe-25" in Paris (France).

REFERENCES

[1] A.P. Buslaev, D.A. Kuchelev, M.V. Yashina, “Dynamic systems and mathematical models of information traffic,” *T-Comm*. 2018. Vol. 12. No. 3. Pp. 22-38.

[2] S.V. Kozlov, A.N. Kubankov, “Process foundations of integration and comprehensive development of information, control, robotic, telecommunication systems,” *High-Tech in Earth Space Research*. 2020. Vol. 12. No. 1. Pp. 23-31.

[3] V.A. Dokuchaev, V.V. Maklachkova, V.Yu. Statev, “Classification of personal data security threats in information systems,” *T-Comm*. 2020. Vol. 14. No. 1. Pp. 56-60.

[4] A.N. Burenin, K.E. Legkov, “Security issues of infocommunication systems and special-purpose networks: main threats, methods and means of ensuring comprehensive network security,” *High-Tech in Earth Space Research*. 2015. Vol. 7. No. 3. Pp. 46-61.

[5] R.I. Zakharchenko, I.D. Korolev, “Methodology for assessing the sustainability of critical information infrastructure facilities operating in cyberspace,” *High-Tech in Earth Space Research*. 2018. Vol. 10. No. 2. Pp. 52-61.

[6] D.S. Chirov, E.M. Lobov, “Selection of a signal-code design for a command-telemetry radio communication line with medium- and long-range unmanned aerial vehicles,” *T-Comm*. 2017. Vol. 11. No. 10. Pp. 21-28.

[7] O.G. Chertova, D.S. Chirov, “Construction of a backbone communication network based on small-sized unmanned aerial vehicles in the absence of ground infrastructure,” *High-Tech in Earth Space Research*. 2019. Vol. 11. No. 3. Pp. 60-71.

[8] A.N. Burenin, K.E. Legkov, V.V. Orkin, “Algorithm for adaptive control of information systems under conditions of mass disturbances,” *High-Tech in Earth Space Research*. 2017. Vol. 9. No. 6. Pp. 90-95.

[9] I.V. Bogachkov, “Detection of strained sections in optical fibers based on the Brillouin reflectometry method,” *T-Comm*. 2016. Vol. 10. No. 12. Pp. 85-91.

[10] D.S. Chirov, E.O. Lobova, “Wideband hf signals dispersion distortion compensator based on digital filter banks. Theory and approbation,” *T-Comm*. 2020. Vol. 14. No. 4. Pp. 57-65.

[11] A.S. Kryukovsky, D.S. Lukin, D.V. Rastyagaev, Yu.I. Skvortsova, “Numerical modeling of the propagation of spatio-temporal frequency-modulated radio waves in an anisotropic medium,” *T-Comm*. 2015. Vol. 9. No. 9. Pp. 40-47.

[12] S.S. Dymkova, “Identifying and implementing successful scientific projects, in the framework of 'IEEE technology and engineering management society' events,” *2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020*. Proceedings. New York, 2020. Pp. 9261533.

[13] O. Varlamov, “Research of influence of DRM broadcast transmitter nonlinearities onto the output signal parameters,” *T-Comm*. 2014. Vol. 8. No. 2. Pp. 59-60.

[14] V. Tikhvinskiy, E. Deviatkin, A. Aitmagambetov, A. Kulakaeva, “Provision of IoT services for Co-Located 4G/5G networks utilization with dynamic frequency sharing,” *2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020:* Proceedings, Vienna, October 20-22, 2020. P. 9261526. DOI 10.1109/EMCTECH49634.2020.9261526.

[15] A. Pastukh, V. Tikhvinskiy, S.S. Dymkova, O.V. Varlamov, “Challenges of using the l-band and s-band for direct-to-cellular satellite 5G-6G NTN systems,” *Technologies*. 2023. Vol. 11. No. 4. Pp. 110.

[16] Pastukh A., Deviatkin E., Tikhvinskiy V., Kulakaeva A., “Compatibility studies between 5G IoT networks and fixed service in the 6425-7125 MHz band, “*2021 International Conference on Engineering Management of Communication and Technology, EMCTECH* 2021 – Proceedings. 2021. DOI: 10.1109/EMCTECH53459.2021.9619176.

[17] A. Pastukh, V. Tikhvinskiy, E. Devyatkin, A. Kulakayeva, “Sharing studies between 5G IoT networks and fixed service in the 6425-7125 MHz band with Monte Carlo simulation analysis”, *Sensors*. 2022. Vol. 22. No. 4. DOI: 10.3390/s22041587.

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

CYBERSECURITY EDUCATION: SYSTEMS APPROACH

Angelina Bott [1]

[1] Institute of Radio and Information Systems (IRIS), Vienna, Austria;

iris@media-publisher.eu

ABSTRACT

This research paper looks at existing research in national cybersecurity education capacity and explores the application of a "systems approach" to guide future cybersecurity education capacity development, using systems thinking tools to build a holistic understanding of the national cybersecurity education capacity landscape. To close the global cybersecurity workforce gap and continue institutionalizing an approach to a structured process for a cybersecurity workforce, it is important to further develop national cybersecurity education capacity in all countries around the world. This research paper is aimed at stakeholders working across government, private sector, academia, and civil society that are interested in how a systems approach can improve the understanding of national cybersecurity education landscapes and guide the design and implementation of future capacity development interventions, with particular application to low-and-middle income countries. Informed by secondary sources, this paper intends to initiate a broader discussion and further research on the benefits and applications of a systems approach to cybersecurity education capacity development.

DOI: 10.36724/2664-066X-2024-10-5-47-66

Received: 25.09.2024
Accepted: 20.10.2024

Citation: Angelina Bott, "Cybersecurity education: systems approach" *Synchroinfo Journal* **2024**, vol. 10, no. 5, pp. 47-66

KEYWORDS: *cybersecurity education, national education capacity development*

The article was prepared based on the materials of "A systems approach to understanding national cybersecurity education capacity", 2024. https://www.itu.int/hub/publication/d-phcb-cyb_educ-2024/

1 Introduction

The International Telecommunication Union (ITU) has a long-standing history of collaboration with the Organization of American States (OAS) on digital transformation initiatives. Both ITU and OAS prioritize a human-centric approach to digital transformation, recognizing that sustainable and resilient ICTs depend on people equipped with the necessary skills and knowledge to manage and operate technology. This framework, designed to help countries understand and navigate their unique cybersecurity ecosystems, emerged from the recognition of the need for a more comprehensive approach to cybersecurity capacity development. By fostering a deeper understanding of the cybersecurity education ecosystem, this approach aims to balance immediate workforce gaps with long-term requirements, ensuring sustained cybersecurity resilience. By leveraging this framework, countries can make strategic investments in their cybersecurity workforce, fostering collaboration between stakeholders to bridge skills deficits and optimize resource allocation.

A review of five leading frameworks for assessing national cybersecurity capacity identified five components of national cybersecurity education capacity: including School Curricula and Programs, Tertiary Education and Research, Training and Certification, Awareness and Culture, and Administration and Governance.

Supply-side challenges

• Lack of awareness and aspiration for cybersecurity careers and unclear career pathways.

• Underutilization of full labor market potential.

• Need to increase the accessibility of a range of cybersecurity education and training pathways.

• Need for greater alignment of cybersecurity education competencies with industry needs.

• Difficulties encountered for education offerings to keep up to date due to rapid pace of change in cybersecurity.

• Lack of educator expertise and resources to deliver cybersecurity education at scale.

Demand-side challenges

• Demand for cybersecurity competencies is rapidly growing and outpacing supply, not just for building a cybersecurity workforce, but for building a cybersecure society.

• Cybersecurity workforce requirements vary by country context, with different needs, environments, cultures, and resources influencing cybersecurity education.

• Need for greater clarity in defining and communicating cybersecurity industry requirements for labor.

• High entry-level requirements for cybersecurity roles make it difficult for aspiring professionals to enter the cybersecurity workforce.

• Employers' underinvestment in the necessary resources and ongoing training of cybersecurity workforce.

Adaptations of a select set of tools to the problem of low national cybersecurity education capacity are presented to explore their utility in building a holistic understanding of the system. A Problem Tree provides a high-level visual representation of some of the causes and effects of the problem of low levels of cybersecurity education capacity. The Stakeholder Analysis provides an indicative list of stakeholders and maps their varying levels of interest and roles in national cybersecurity education capacity. The Systems Concept provides a high-level representation of national cybersecurity education capacity as a system. The system concept takes into consideration the five components of national cybersecurity education capacity identified in this paper and situates them within the context of the overall system environment, illustrating potential interrelationships between the system components.

Cybersecurity continues to be a key challenge to the ongoing stability, safety, and productivity of the global economy. Without interventions now, it will be difficult to maintain the integrity of and trust in the emerging technology on which future global growth depends. Despite advancements in cybersecurity education and other capacity development activities, a persistent disparity of low supply and high demand exists in the global cybersecurity workforce. The geo-political landscape, ongoing economic digital transformation efforts, and uncertainties around emerging technologies such as AI have all contributed to an evolving digital risk and threat environment that places pressure on the resiliency and efficacy of cybersecurity workforces [1].

The International Information System Security Certification Consortium, Inc. (ISC2) estimated in 2022 that the global cybersecurity workforce had reached 4.7 million people and that the world needed a further 3.4 million cybersecurity professionals to cope with the growing number of threats and challenges [2]. Cybersecurity workforce challenges are more acute in low- and middle-income countries where limited resources are stretched across a range of policy priorities, and it is therefore critical to use and deploy available resources efficiently and build on existing capacity as part of the broader development context.

Given the size of the cybersecurity challenge and need for effective investment, there is an opportunity for education and broader digital literacy efforts to play a key role in mainstreaming cybersecurity in national and global development contexts. This can help to facilitate the achievement of the 2030 Agenda for Sustainable Development and provide a driving force for Sustainable Development Goal 4 on quality education [3] by equipping both young people and adults with the knowledge, and technical and vocational skills, to thrive in an increasingly digitalized world [4].

To reduce the global cybersecurity workforce deficit, it is important to further develop national cybersecurity education capacity in all countries around the world. This study looks at existing research in national cybersecurity education capacity and explores the application of a 'systems approach' to guide future cybersecurity education capacity development. A systems approach seeks to address complex policy challenges by using a holistic design methodology, which considers how individual elements work together and how they are impacted in context. This study explores the application of a systems approach to guide future cybersecurity education capacity development by:

• identifying and describing current research on the challenges and characteristics of national cybersecurity education capacity;

• exploring how a systems approach can support the understanding and development of cybersecurity capacity;

• adapting systems thinking tools for consideration in the conceptualization of national cybersecurity education capacity as a system;

• outlining recommendations for national cybersecurity education capacity building.

This study is aimed at stakeholders working across academia, and civil society who are interested in how a systems approach can improve the understanding of national cybersecurity education landscapes and guide the design and implementation of future capacity development.

The analysis of cybersecurity capacity must reflect the diversity of conditions, composition, and priorities of capacity and workforce development goals to determine the suitability of a systems approach to varying national contexts. By exploring the application of a systems approach, stakeholders can draw on these ideas and concepts as part of their efforts to understand and strengthen national cybersecurity education capacity.

2 Review of cybersecurity education capacity

This section presents an overview key elements of existing national cybersecurity education capacity research including academic journals, frameworks and guides, policy and industry papers, and websites. The criteria for the selection of these resources included:

• recency: publication in the last eight years (2016 to 2023);

• diversity of publication type: ensuring diversity of source type by including nine academic journal articles, seven frameworks and guides, and thirteen policy/industry papers, and one research centre website;

• diversity of author: representation of both government and non-government authors;

• diversity of geography, which included authors from Africa, the Americas, Asia-Pacific, and Europe regions.

Building education capacity

This section outlines key considerations when building national cybersecurity education capacity and presents the complexity and multi-faceted nature of capacity building as well as the challenges typically experienced by countries when addressing low capacity. It includes an overview of maturity and readiness indicators drawn from leading cybersecurity capacity assessment frameworks, what a country needs to consider, and the typical stages in the capacity building process.

Despite the progress made over the past decade, national cybersecurity education capacity building is still an emerging field and there is a need for further evidence of what works best in practice and how the global community can assist low- and middle-income countries in building a cybersecurity workforce and cybersecure society.

An understanding of the key challenges faced in building national cybersecurity education capacity can help to support the design and implementation of capacity building measures. This includes the demand-side factors [5-11] (national and organizational need for cybersecurity knowledge, skills, and abilities) and supply-side factors [12-17]. Awareness, education, and training of the cybersecurity workforce and population that need to be addressed and aligned in order to drive holistic improvements, as detailed in Table1 [42].

Table 1

Supply and demand challenges for cybersecurity education capacity

Examples of supply-side challenges	Examples of demand-side challenges
• Lack of awareness and aspiration for cybersecurity career pathways by students. • Lack of clarity of career roadmaps and progression pathways for prospective cybersecurity professionals. • Underutilization of full labour market potential for a cybersecurity workforce, with women severely underrepresented and a need to involve more minority groups in cybersecurity education programmes. • Need to increase the availability and accessibility of a range of cybersecurity education and training pathways including apprenticeships, tertiary, and re-training programmes. • Need for greater alignment of cybersecurity competencies developed through formal education programmes and curricula with industry expectations and needs. • Difficulties encountered for education offerings and curricula to keep up to date due to rapid pace of change in the cybersecurity field. • Lack of educator expertise and resources to deliver required cybersecurity education at scale at secondary and tertiary education levels. • Lack of awareness, limited resources, and governance capacity to address cybersecurity capacity in the context of competing national development priorities.	• Demand for cybersecurity competencies is rapidly growing and outpacing supply not just for building a cyber- security workforce, but for building a cybersecure society. • Cybersecurity workforce requirements vary by country context, with different needs, environments, cultures, and resources influencing cybersecurity education design and availability. • Need for greater clarity and building capability for organisations to define and communicate cybersecurity industry requirements for labour and recognizing cybersecurity as its own profession rather than a sub-set of IT roles. • High entry-level requirements for cybersecurity roles make it difficult for aspiring cybersecurity professionals to enter the cybersecurity workforce. • Employers' underinvestment in the necessary resources and ongoing training of cybersecurity workforce.

Indicators of commitment, maturity and readiness

In order to address the supply and demand challenges there is an urgent need for a national cybersecurity education strategy that bolsters multiple initiatives as well as a multi-stakeholder space in which government, industry, and academia can actively work together to address national cybersecurity educational requirements.

The components and indicators of national cybersecurity education capacity need to be understood, and the following five leading frameworks outline some important indicators to measure and build capacity:

• Global Cybersecurity Index (GCI) [18] developed by ITU covers capacity building measures.

• National Cyber Security Index (NCSI) [19] developed by the e-Governance Academy Foundation, includes two indicators: cyber safety and security website, and education and professional development.

• National Capabilities Assessment Framework (NCAF) [20] developed by the European Union Agency for Cybersecurity (ENISA), covers capacity-building and awareness.

• Cybersecurity Capacity Maturity Model for Nations (CMM) [21] developed by the Global Cyber Security Capacity Centre (GCSCC) covers “Building cybersecurity knowledge and capabilities”.

• Cyber Readiness Index (CRI) [22] developed by the Potomac Institute for Policy Studies covers investment in research and development (R&D).

A review of these five frameworks identified the following five main components:

• school curricula and programmes;
• tertiary education and research;
• training and certification;
• awareness and culture;
• administration and governance.

Each of these five components have specific indicators initiated and driven by stakeholders in the public, private, and civil society sectors.

Elements of the school curricula and programmes component include:

• incorporating cybersecurity and cyber safety as a part of the school curriculum;
• building aspirations for cybersecurity career paths including the introduction of games, competitions, informational talks, and technology demonstrations;
• identifying stakeholders at the school level beyond students, to include teachers, parents, administrators, and other relevant community members to engage in related initiatives;
• ensuring that primary and secondary schools have qualified cybersecurity teachers "Cybersecurity education capacity features of the school curricula and programmes component drawn from" [23-26].

Elements of the tertiary education and research component include:

• offering cybersecurity as part of a suite of tertiary education programmes such as diplomas, bachelor degrees and masters, and PhD pathways, which should include specialist cybersecurity programmes and involve cybersecurity in other technical and non-technical subject areas such as computer science, engineering, business, finance, healthcare, law, and public policy;
• ensuring cybersecurity curricula keeps up to date with research and developments in the field;
• developing a national certification programme for the accreditation of cybersecurity programmes;
• offering alternative cybersecurity education pathways, including vocational colleges and trade-apprenticeships;
• encouraging tertiary education providers and industry to work together to ensure cybersecurity education programmes align with cybersecurity workforce needs and wherever possible incorporate work-based learning and work integrated learning as part of the curricula;
• ensuring the supply of cybersecurity subject area qualified academics at the tertiary level;
• encouraging industry and government experts to participate in cybersecurity education delivery;
• establishing cybersecurity research centres;
• establishing and encouraging formal and informal public-private partnerships that drive cybersecurity research and development programmes "Cybersecurity education capacity features of the tertiary education and research component drawn from" [27-28].

Work integrated learning

Work integrated learning (WIL) is an educational approach that integrates practical work experience as part of the curricula. This approach provides students with opportunities to turn theory into practice and gain real-world experience. This combination of academic study and practical experience helps students develop a broad range of skills and competencies as well as creating opportunities for mentorship and networking with industry. As cybersecurity is a rapidly evolving field where applied skills and up-to-date knowledge are highly valued, WIL can provide students with the opportunity to work with real cyber threats and security challenges, enabling them to develop vital problem-solving skills and an understanding of how to handle real-world cybersecurity incidents.

WIL can take a variety of forms including work placements, fieldwork, industry projects, and internships. For example, Western Sydney University in Australia offers a Bachelor of Cyber Security and Behaviour course where final year students complete 44 days as an intern in a cybersecurity related workplace. During this time students complete a range of related assessments such as a journal on what they have learnt, assignments based on their role, and feedback from supervisors. This experience provides the student with credit for the equivalent of four full subjects of study towards their certification [29, 30].

Elements of the training and certification component include:

• availability and accessibility of a range of cybersecurity training courses including in technical and non-technical areas; for experts and non-experts; formal and informal learning and mentoring; and aimed at operational and executive levels;

• availability and accessibility of cybersecurity professional certifications;

• availability of cyber exercises and drills at the regional, national, sectoral, and organizational level;

• availability of cybersecurity mentorship programmes;

• existence of cybersecurity professional associations;

• existences of a register of certified cybersecurity professionals in the country.

Cybersecurity Education Capacity features of the Training and Certification component drawn from [31].

Elements of the awareness and culture component, include Cybersecurity Education Capacity features of the Awareness and Culture component drawn from:

• formal and informal cybersecurity awareness programmes that build a cybersecurity culture in government, industry, academia and civil society and which include elements such as the promotion of digital literacy and cyber safety skills, highlighting cybersecurity risks, developing cybersecure work practices, and encouraging participation in the cybersecurity workforce;

• targeted cybersecurity executive awareness programmes adapted for different sectors of the economy such as finance, telecommunications, critical infrastructure, and government agencies;

• availability and accessibility of an online portal and resources to provide cybersecurity information to the general public as well as government, industry, academia and civil society.

Elements of the administration and governance component, include Cybersecurity Education Capacity features of the Administration and Governance component drawn from [32]:

• incorporating capacity and workforce development as part of national strategies and policies, including broad consultation with government, private sector, academia and civil society stakeholders;

• developing of a national cybersecurity education and research action plan;

• designating at least one government entity to oversee the implementation, monitoring and evaluation of the national cybersecurity education action plan;

• allocating government resources to fund cybersecurity education capacity development programmes;

• adopting a common taxonomy for government, industry, and academia to describe cybersecurity workforce requirements and share information, knowledge, skills, and abilities;

• ensuring regular engagement and cooperation between government, education providers and industry to align supply and demand requirements of the cybersecurity workforce.

These elements can be supported by the introduction of government funded incentive mechanisms such as:

• promotion of competitions and other initiatives that drive aspirations for cybersecurity careers;

• funding targeted programmes for underrepresented groups such as women to ensure the full inclusion of the available workforce;

• grants to encourage the transition to cybersecurity careers;

• grants to encourage the retention of the cybersecurity workforce within the country;

• cybersecurity education programme scholarships;

• cybersecurity R&D tax credits, grants and scholarships.

Building capacity

To effectively address the supply and demand challenges to build capacity, it is important to adopt a holistic approach when raising the level of maturity and readiness of existing cybersecurity education capacity (taking the various components into account). The European Commission [33] provides a framework for such an approach as part of the 'Operational Guidance for the EU's International Cooperation on Cyber Capacity Building' in which all cybersecurity capacity development efforts must be built across individual and organizational capacity, and the enabling environment (Table 2) [42].

Table 2

Levels of capacity

Individual capacity	Organizational capacity	Enabling environment
Capacity building for individuals is the process of equipping them with the understanding, skills and access to information, knowledge and training to perform effectively.	Capacity building for an organization is focused on the elaboration of management structures, processes and procedures internally and managing relationships between different organizations and sectors (public, private and community).	Creating an enabling environment is about generating the right set of legal, regulatory, economic and societal changes that ultimately support organizations, institutions and agencies at all levels and in all sectors in enhancing their capacities.

Stages of cybersecurity capacity building

The Operational Guidance for the EU's International Cooperation on Cyber Capacity Building also defines the main stages of capacity building as part of its proposed Cyber Capacity Building Framework (CCBF). The checklist for cybersecurity capacity-building stages, detailed below and illustrated in Figure 1, provides a process that countries can apply in the preparatory stages to achieve their capacity building goals.

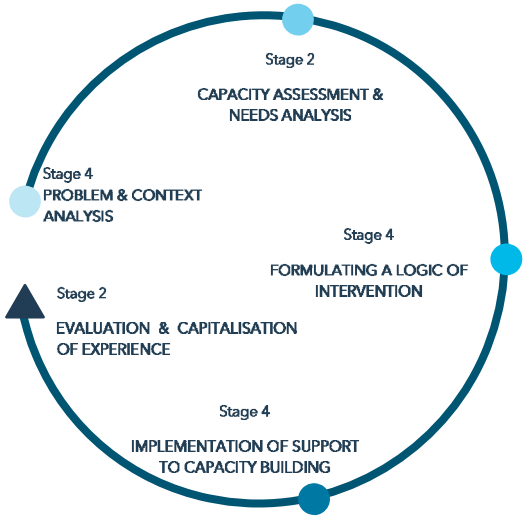


Fig. 1. Cybersecurity capacity building stages [42]
Source: adapted from the EU operational guidance

• Problem and context analysis: Understanding the problem to be addressed, the broader context and strategic drivers, and defining capacity building goals.

• Capacity assessment and needs analysis: Understanding existing capacities, resources available, and the identification of the gaps and priorities.

• Formulating a logic of intervention: Identifying specific agents of change, capacities to be strengthened, as well as any moderating factors that can impact success.

• Implementation of support to capacity building: Facilitating and monitoring the delivery of the intervention.

• Evaluation and capitalization of experience: Assessment of the achievement of the capacity building goals and lessons to support future actions.

3. Systems approach to education capacity building

The systems approach concept

The findings outlined in section 2 reveal the complex and multi-faceted issues when seeking to determine the state of maturity, address gaps, develop national cybersecurity capacity and build resilience in their cybersecurity ecosystem. This complexity, and the ever-changing environment, makes cybersecurity education a so-called 'wicked problem', one that requires a holistic and multi-level response given its critical function as a part of the solution. The challenges of national cybersecurity education capacity have been summarized by Bate when describing experiences in the United States of America:

This section outlines the potential merits of applying a systems approach that seeks to address the complex policy challenges using a holistic approach, which includes understanding how individual elements work together, how elements are related, and how they are impacted by their environment. A systems approach requires a diverse range of perspectives to understand the various inputs, processes, and outputs of the system.

Allen and Kilvington [34] identify four key components of a systems approach to address a 'wicked' problem. These components include:

1 Multiple perspectives: who are the key actors that are part of or impacted by the situation and how do their knowledge systems and views frame their perspectives and level of engagement with the issues?

2 Interconnections: how do the various elements of the system interconnect, what are the patterns of these connections and the nature and direction of these relationships?

3 Boundaries: what is the scope and scale of the system, and how do different actors consider definitions of and improvements to the problem being addressed?

4 Influence: what are the enablers and barriers within a system, what drives the system and what are the leverage points that offer the greatest potential for intervention to influence system outcomes?

There is merit in breaking down complex systems to a level of abstraction that allows for a deeper understanding of which components are important and how they might be interacting with each other to produce a given result. This is explained further by the Organization for Economic Co- operation and Development (OECD) [35], which identified education as a public sector challenge that could benefit from a systems approach.

Why consider exploring a systems approach for national cybersecurity education capacity? Given the importance and complex nature of national cybersecurity education capacity building and the limited resources available to governments, a systems approach offers the potential to assist governments and other relevant actors to optimize their response to this challenge. Establishing a holistic understanding of the key elements and boundaries of the national cybersecurity education capacity building system can help governments to identify existing and future actions that will drive positive change in the system. Furthermore, by identifying interrelationships between different elements, governments can begin to understand how actions and investments in one component of national cybersecurity education capacity may impact others, and whether the impact is likely to be positive or negative [36].

Greater understanding of the national cybersecurity education capacity system can create a shift in policy approach. This can be achieved by recognizing that the individual elements of the system can act differently when in isolation or as a part of the wider system. This can help governments to provide a framework to identify key leverage or primary intervention points where targeted activity might help to optimize and nurture the capacity of the system. Such an approach has the potential to increase the efficacy of cybersecurity education capacity actions, optimize resource allocation, and drive long-term positive impacts and the achievement of policy goals over time.

The following section explores how applying a systems approach to a problem aligns with existing frameworks on national cybersecurity capacity building processes.

Systems approach to capacity building

Consistent with capacity building in a project and programme management cycle, a structured process can also be followed when applying a systems approach to a problem. This helps to define the components of a system and offer solutions. Allen and Kilvington introduce this process through a systemic design cycle that consists of three functions: understand the system, co-design solutions, and assess and adapt. These functions should be underpinned by ongoing dialogue and collaboration between key system stakeholders. This systemic design cycle is illustrated in Figure 2.

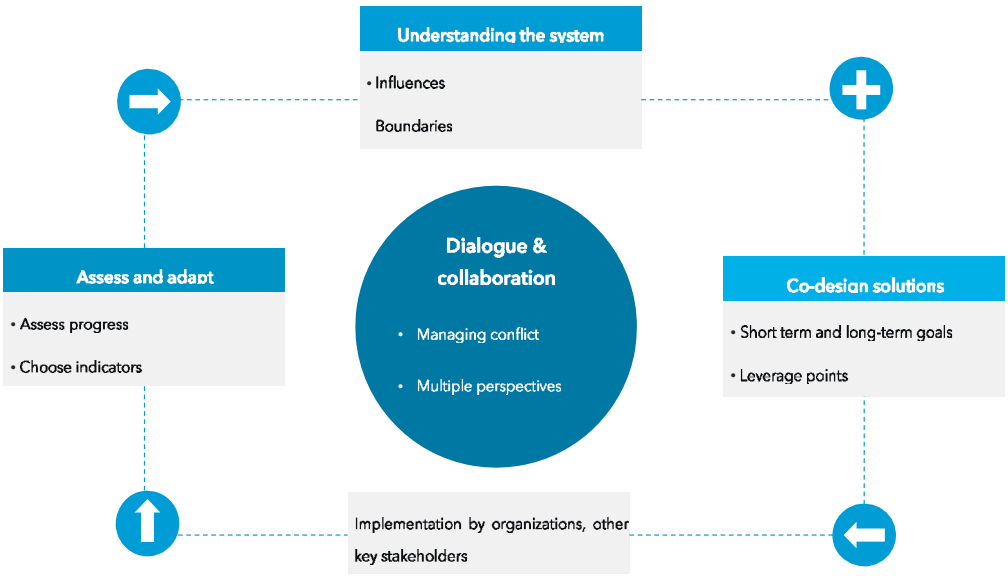


Fig. 2. Systemic design cycle [42]
Source: adapted from Allen and Kilvington "Key systems thinking components"

The systemic design cycle has parallels with the project and programme management cycle. Table 3 aligns these approaches for cybersecurity capacity building.

Table 3

Alignment of approaches

Stage	Cybersecurity capacity building in the project and programme management cycle	Systemic design cycle functions	
1	Problem and context analysis	Understanding the system	Dialogue & collaboration
2	Capacity assessment and needs analysis		
3	Formulating a logic of intervention	Co-design solutions	
4	Implementation, including monitoring and reporting	Implementation by organizations, other key stakeholders	
5	Evaluation of the provided support	Assess and adapt	

Mapping the systemic design cycle functions to cybersecurity capacity building in the project and programme management cycle, makes it easier to identify the types of systems thinking tools that might most benefit policy-makers and educators in their cybersecurity education capacity building efforts. Examples of systemic design function tools [37, 38] that may be useful as part of this process include:

• Iceberg models assist in understanding complex issues by looking beyond surface level events to understand the range of patterns, structures, and mental models influencing the situation being assessed.

• Logic models provide a visual representation of how an initiative is expected to perform by detailing the connections and flow between inputs, change mechanisms, outputs, outcomes, impacts and moderating factors.

• PESTLE analysis is a strategic framework to analyse the political, economic, social, technological, legal, and environmental (PESTLE) factors in which an intervention is being deployed.

• Problem and objective tree is a set of visual tools that can illustrate relationships and connections. A problem tree can assist in identifying the root causes of a problem and its consequences. An objective tree is a complementary tool which uses the causes and effects of the problem tree and reverses them to identify objectives and outcomes to solve the problem.

• Stakeholder analysis or mapping is used to identify and understand the range of individuals, groups and other entities that are likely to have an interest in, be affected by, or have the ability to influence the success of an initiative.

• System concept mapping is visualization tool to represent and allow for the analysis of complex systems through identifying and illustrating system components, relationships and feedback loops.

Three of these tools have been selected and applied to the problem of national cybersecurity education capacity in section 4: problem trees, stakeholder analysis, and systems concept mapping.

4. Understanding the cybersecurity education capacity system

There are a wide range of tools to help policy-makers and practitioners explore systems approaches to policy challenges. This section sets out how a select set of tools can be adapted to national cybersecurity education capacity and explores how they can be used to build a holistic understanding of the system. The application of these tools depends on the different national contexts in which they are used and this section introduces general concepts as the basis for future discussion. It is important to note that the tools presented here should be adapted to each country's policy goals and individual system characteristics.

Problem tree

The national cybersecurity education capacity system problem tree, illustrated in Figure 3, is an example of a systems tool that leads to an understanding of the system by identifying the components and how they connect.

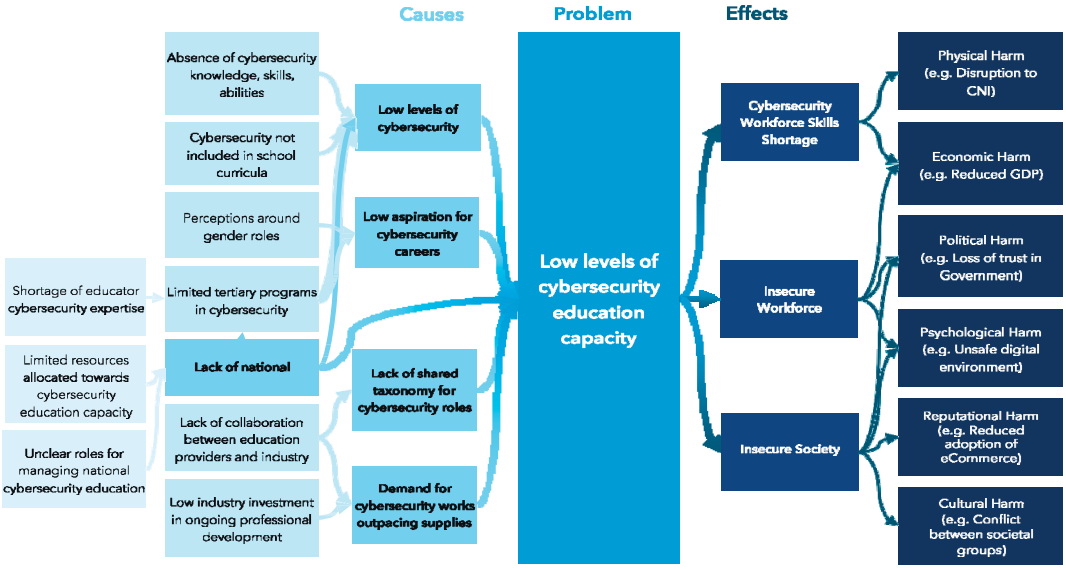


Fig. 3. National cybersecurity education capacity problem tree [42]
Source: ITU

For national cybersecurity education capacity building, the decision tree presents some of the causes and effects of low levels of cybersecurity education capacity [39]. It incorporates insights from the challenges identified in section 2 and shows how low levels of national cybersecurity education capacity can lead to negative effects.

Stakeholder analysis

The stakeholder analysis tool assists in building a deeper understanding of national cybersecurity education capacity. As stakeholders are likely to have different perspectives, interests, and power over systems and how they work, it is important to gather multi-stakeholder perspectives to reach a holistic understanding of the system. Table 4 provides an indicative list of stakeholders with varying levels of interest and roles in national cybersecurity education capacity.

Table 4

National cybersecurity education stakeholders

Stakeholder	Type	Interests/roles in national cybersecurity education capacity
School students	Individual	• Students at primary and secondary education levels have the opportunity to engage in cybersecurity related academic and aspiration building learning and activities.
Tertiary students	Individual	• Students at tertiary level may be actively pursuing cybersecurity as a career path and look to obtain knowledge, skills, and abilities to enter the workforce. • Other students at this level may benefit from cybersecurity knowledge as part of their studies in areas other than cybersecurity e.g., computer science, engineering, business, finance, healthcare, law, and public policy.
Parents	Individual	• Parents of primary, secondary and tertiary level students will have varying levels of engagement in the academic achievement and career aspirations of their children and may influence decisions to pursue cybersecurity careers.
School teachers	Individual	• School teachers have a direct role in delivering cybersecurity related curricula and activities and can play a key role in the future education and career direction and development of their students.
Tertiary educators	Individual	• Tertiary educators have a direct role in delivering cybersecurity related curricula and activities and can play a key role in the future education and career direction and development of their students.
General public	Individual	• Individual members of the general public will require an understanding of cybersecurity and the tools to keep them safe online.
National governments	Government	• National governments set policy directions and resource allocations for the achievement of cybersecurity education and workforce development goals, as well as broader national security responsibilities to protect individual citizens, organizations, government systems and national infrastructure.
Government agencies	Government	• Government agencies administer allocated resources to achieve national cybersecurity workforce and national security policy goals. • Government agencies also contribute to demand for the cybersecurity workforce. • Government agencies develop and implement specific actions to achieve policy goals.
Private sector	Private	• The private sector drives demand for the cybersecurity workforce and typically leads the way in knowledge, skills, and ability requirements for the cybersecurity professionals. • The private sector invests resources to support their own workforce requirements and engagement with other stakeholders to achieve workforce goals. • The private sector has an interest in informing government policy development and implementation. • The private sector also often plays a leading role in cybersecurity education through academies and training programmes.
Civil society	Civil society	• Civil society also drives demand for the cybersecurity workforce. • Civil society has an interest in informing government policy development and implementation.

Research centres	Education	• Research centres support research and development and look for opportunities for commercialization of cybersecurity innovations. • Research centres help to identify opportunities and threats that may affect government, private sector, and civil society stakeholders and society.
Professional training providers	Education	• Professional training providers offer courses to support certification and professional development of the cyber- security workforce and other training needs including both technical and non-technical training at both operational and executive levels. • Professional training providers have interests in government, private sector and civil society workforce needs. • Professional training providers have an interest in supporting government policy development and implementation.
Universities and trade colleges	Education	• Universities and trade colleges offer formal programmes in cybersecurity and also have the opportunity to embed cybersecurity skills across a broad range of programme areas. • Universities and trade colleges have interests in government, private sector and civil society workforce needs. • Universities and trade colleges have interest in informing government policy development and implementation. • Universities and trade colleges work with schools, employers, and governments on
Primary and secondary schools	Education	ti b it th • Primary and secondary schools facilitate opportunities to teach cybersecurity and related curriculum and run related activities. • Primary and secondary schools may work with trade colleges, universities, employers, and government to promote different career pathways.

Figure 4 maps the stakeholders listed in Table 4 based on estimated levels of interest and power regarding the building of national cybersecurity education capacity [40, 42]. For the purpose of this exercise, 'Interest' considers to what degree each stakeholder is likely to be affected by changes in national cybersecurity education capacity, and how much they are interested or concerned. 'Power' considers the influence they may have over national cybersecurity education capacity building, and to what degree they can help to achieve, or block, the desired change.

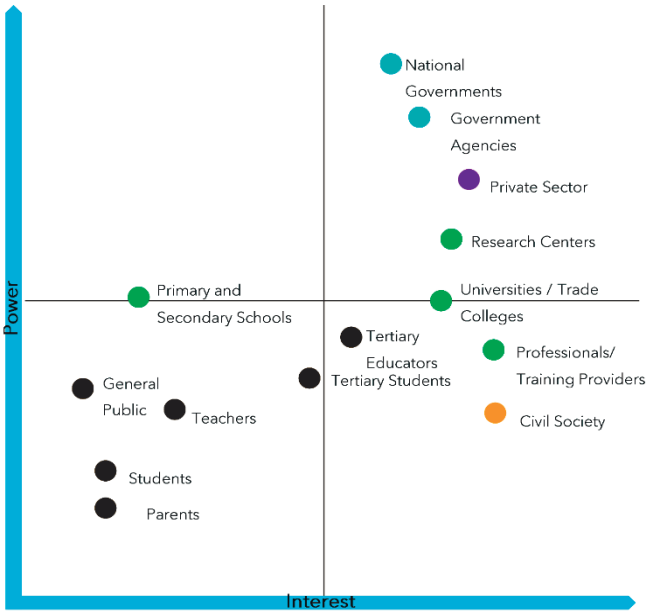


Fig. 4. National cybersecurity education capacity stakeholder map [42]

System concept

Figure 5 provides a high-level representation of national cybersecurity education capacity as a system.

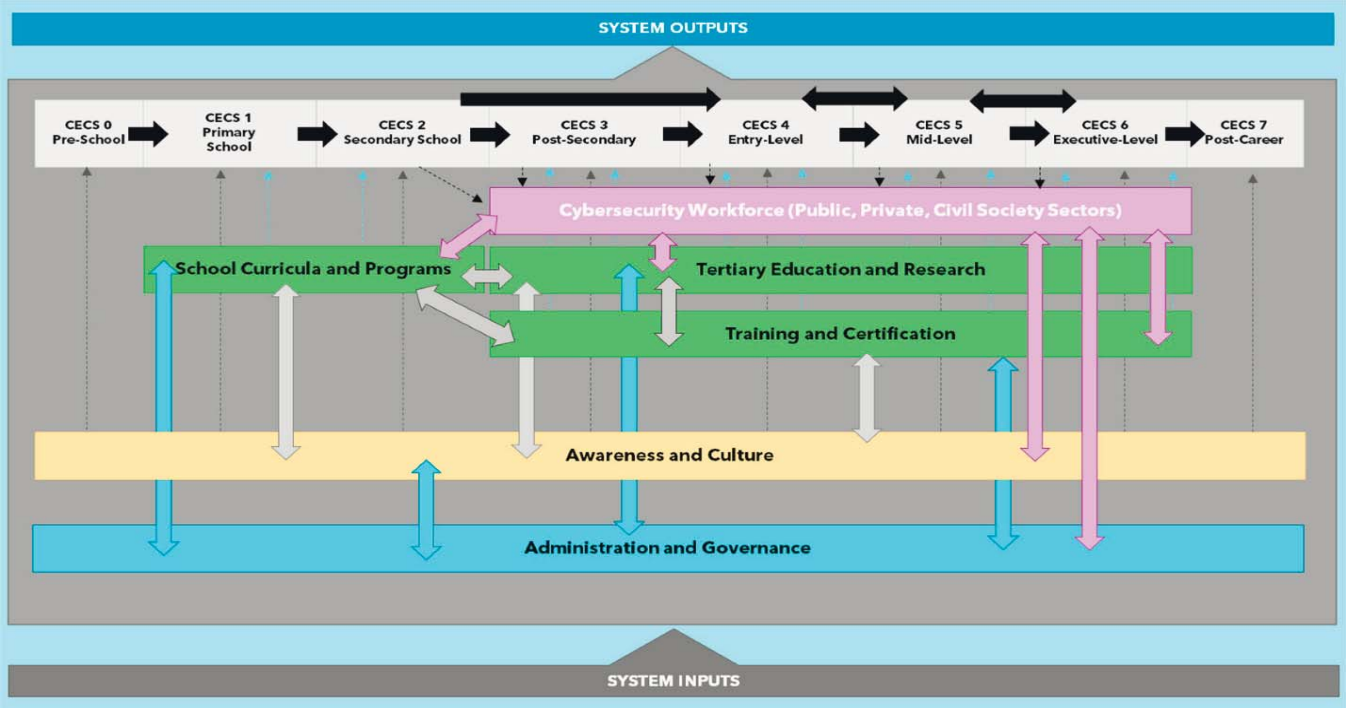


Fig. 5. National cybersecurity education capacity system concept [42]

Table 5

Key to systems concept in Figure 5

Colour and shape	Description
Light blue box	The area within this box represents the national cybersecurity education capacity systems environment e.g. represents all the various cybersecurity and wider societal components of a country.
Grey box	This box contains the boundary of the national cybersecurity education capacity system.
Blue box	This box contains the outputs of the national cybersecurity education capacity system.
Dark blue box	This box contains the inputs of the national cybersecurity education capacity system.
Lighter blue box	This box contains the administration and governance component of national cybersecurity education capacity.
Yellow box	This box represents the awareness and culture component of national cybersecurity education capacity.
Green box	These three boxes represent the school curricula and programmes, tertiary education and research, and training and certification components of national cybersecurity education capacity. These three components have been grouped together as they represent opportunities for facilitating the direct transfer of cybersecurity knowledge, skills, and abilities.
Purple box	This box represents the active national cybersecurity workforce.
Light grey box	These boxes represent the proposed cybersecurity education capacity stages (CECS) that cybersecurity professionals move through as part of the education lifecycle, with the number and characteristics of stages likely to vary between countries.
Solid-black arrows	These arrows indicate the typical direction of travel through the various CECS.
Solid-coloured arrows	These solid-coloured arrows indicate the potential existence and direction of relationships between system elements.
Dotted-coloured arrows	These dotted coloured arrows indicate the direct engagement and potential transfer of knowledge, skills, and abilities, between components of national cybersecurity education capacity and individuals moving through each CECS.
Dotted-black arrows	The dotted black arrows indicate labour force movement from each CECS into the cybersecurity workforce.
Dark grey arrow	This arrow represents inputs into the system e.g., resources, people, technology etc.
Grey arrow	This arrow represents outputs produced by the system e.g. a reduction in cybersecurity harms and a more resilient cybersecure society.

Breaking down the systems concept diagram

The national cybersecurity education capacity system reflects all the components and elements that contribute to national cybersecurity education capacity including activities driven by the public and private sectors, civil society stakeholders and individuals. To ensure the accessibility and comprehension of the system, a high-level abstraction has been presented to allow countries to think about the overall components, interactions, and goals of a system. At this high-level of abstraction, system components include school curricula and programmes, tertiary education and research, training and certification, awareness and culture, administration and governance. In addition to these components, the system includes the cybersecurity workforce and the various cybersecurity education capacity stages (CECS) that interact with each other as well as the five components detailed above. It is these components and how they interact and influence each other that make up the national system. To understand and explore such a national system, it is important to create system boundaries to see how different inputs influence the internal functions of the system and examine how external influences stemming from the system environment impact its dynamics.

The system environment represents the context of the national cybersecurity education capacity system. This includes other areas of significance for national cybersecurity, and the broader range of priorities, challenges, and circumstances that create the conditions in which national cybersecurity education capacity functions. It is important to acknowledge the complex moderating factors that will impact national cybersecurity education, which exists in a broad national, regional, and global environment alongside a vast array of other systems each with their own complexity and impact on each other (e.g., financial system, climate change and environment, food security, transport, social and economic structures, and political systems).

System inputs, represented by the dark grey arrow, influence the operation and sustainability of a system. For a national cybersecurity education capacity system, inputs might include:

- financial and human resources to develop and expand the scale of cybersecurity education;
- technology to facilitate cybersecurity education, including support infrastructure, as well as hardware and software;
- curriculum and training resources that can be adapted and implemented to improve the effectiveness of cybersecurity education;
- knowledge and expertise from cybersecurity experts, practitioners, and systems analysis that can support the design and optimization of national cybersecurity education capacity;
- regional and global cybersecurity factors and other conditions such as changes to the cybersecurity threat landscape and cybersecurity education policies and priorities.

System outputs, represented by the grey arrow, illustrate the product of the system inputs working together to produce outcomes and might include:

- improved sustainability and resilience of the cybersecurity workforce, cybersecure workforce, and cybersecure society, that reflect national priorities and requirements;
- mitigation of cybersecurity risks and harms;
- improved national cybersecurity capacity maturity;
- lessons and knowledge from research and analysis of the system that can provide feedback to improve future performance and optimize policy recommendations to enhance the system.

Cybersecurity education capacity stages

The systems concept introduces the stages of cybersecurity education capacity building as a customizable way to map the education lifecycle of cybersecurity professionals in any given country. The stages are intended to represent the path an individual would follow throughout their education and workforce journey from early childhood to retirement. By deconstructing the cybersecurity education capacity system into smaller, more manageable stages, the aim is to enhance understanding of effective actions needed to reach national cybersecurity education goals. Additionally, this approach is expected to shed light on the interplay of measures across each component of the cybersecurity education capacity system.

The solid-black arrows (⬆) represent the direction that individuals within the system travel between each stage. The direction and movement between each stage may be different for each country and should be customized to align to the typical experience of each country.

The dotted-black arrows ( ) represent the typical timing of when people enter the cybersecurity workforce. This can be customized for each country to highlight when individuals are entering the cybersecurity workforce and where there may be gaps in the system.

As an example, a country might define each CECS as follows:

- CECS 0 – Pre-school
- CECS 1 – Primary school
- CECS 2 – Secondary school
- CECS 3 – Post-secondary
- CECS 4 – Entry-level
- CECS 5 – Mid-level
- CECS 6 – Executive-level
- CECS 7 – Post-career

It should be noted that an individual at any stage can engage with any of the components of the national cybersecurity education capacity system. For example, a full-time university student at CECS 3 may study for a degree in cybersecurity (tertiary education and research component) at the same time as someone who is mid-career in CECS 5. As such, each stage is intended to represent the main study or employment focus of an individual at any given point.

When applying this systems concept to a specific country, the number and characteristics of each stage can be defined to align with existing constructs and contexts (e.g., existing school systems and commonly accepted career levels). Each stage could then be explored taking into account key stakeholders, policy success indicators, moderating factors, and existing actions and resource allocations. This is further explored in Table 6 [42].

Table 6

CECS 2 – Example secondary school characteristics

CECS descriptors	**CECS 2 - Secondary school**	
Key stakeholders	• students (aged 13 to 18) • parents • school teachers • secondary schools	• universities • trade schools • government agencies • entry-level employers
Policy success indicators	• numeracy and literacy academic attainment • participation in cybersecurity initiatives • interest in cybersecurity careers • application for tertiary cybersecurity programmes (vocational and university)	
Moderating factors	• school types and resourcing levels • urban and rural digital divide • education attainment of parents • awareness of cybersecurity as a career	
Existing actions and resource allocations	• cybersecurity as a part of secondary school curriculum • teacher cybersecurity training programmes • cybersecurity competitions • national cybersecurity awareness month	

Key system components:

• Coordinating components (light blue box) represent the administration and governance components of national cybersecurity education capacity and interacts with the system by guiding the allocation, intent, and direction of inputs within the system.

• Awareness components (yellow box) represent the awareness and culture components of national cybersecurity education capacity, which focuses on informing stakeholders within the system of the importance, relevance, and scope of cybersecurity.

• Education delivery components (green boxes) include school curricula and programmes, tertiary education and research, and training and certify. These components have been grouped together as they represent opportunities for the direct transfer of cybersecurity knowledge, skills, and abilities that enable recipients to complete cybersecurity related tasks and practices.

The solid-coloured arrows represent the relationships between components. Depending on the country, such relationships may or may not exist, or may only travel in one rather than both directions. This is something that can be customized for each country system concept to help understand how each component influences the operation and effectiveness other components.

The dotted-coloured arrows (light blue, yellow, green) represent how each component directly interacts with individuals in the system as they move through each CECS. This interaction includes the range of cybersecurity aspiration, awareness, knowledge, skill, and ability building activities that exist within a country. This can be customized to show where interaction is most prominent and identify where there might be gaps in the system.

Cybersecurity workforce

The composition of the national cybersecurity workforce represents professionals from all public, private, and civil society sectors and reflects national priorities and requirements, the resources available, and the effectiveness of the national cybersecurity education capacity system.

The purple arrows indicate the relationships between the cybersecurity workforce and the five national cybersecurity education capacity system components, as well as how they impact each other. Depending on the country, such relationships may or may not exist, or may only travel in one rather than both directions.

Considerations for each cybersecurity education capacity stage

Table 6 presents an example of what governments might consider when looking at each stage in the education cycle and potential key stakeholders, policy success indicators, moderating factors, and existing actions and resource allocations as examples of characteristics that could be considered for each CECS. By replicating this process across each identified CECS, policy-makers will be able to develop a comprehensive and holistic understanding of their national cybersecurity education capacity system, including gaps and intervention opportunities.

Application of the systems concept to cybersecurity education capacity building

Looking at national cybersecurity education capacity as a system (as illustrated in Figure 5) can provide planning and implementation benefits for future capacity building measures:

• Goal setting: Assisting government in the formulation of short, medium, and long-term cybersecurity education capacity development and workforce planning by mapping prospective cybersecurity professionals through the different CECS in each country and aligning it to current and future national cybersecurity workforce demand.

• Holistic perspectives: Improving the understanding of system stakeholders and their levels of interests, roles, and influence in relation to national cybersecurity education capacity building.

• Key leverage points: Assisting policy-makers to identify and understand the various leverage or primary intervention points in national cybersecurity education capacity systems that could significantly improve the capacity and outputs of the overall system. This can help resource allocation and focus efforts on points in the system where smaller changes might unlock bigger opportunities in the future. For example, if the cybersecurity education capacity system were to increase awareness of cybersecurity careers in early

secondary school, this might lead to higher levels of engagement and participation in education development pathways, which would in turn increase the overall size of the cybersecurity workforce.

• Effi improvements: Supporting future national cybersecurity capacity building programme design and resource allocation by assisting policy-makers in understanding how investments in certain parts of the system will contribute towards policy goals, and how such investments in one part of the system will interact with existing or proposed measures in other parts of the system. Knowledge of these relationships and leverage points in the system has the potential to improve the effectiveness of the programme as a whole and optimize resource allocations.

• Outcomes and impact: Improving the short-term outcomes and long-term impact of national cybersecurity education capacity building programmes by ensuring that the prioritization of efforts and resources aligns with the needs of the cybersecurity education system and workforce.

Recommendations and conclusion

This study explores the current supply and demand challenges and sets out key components of national cybersecurity education capacity.

This showed how a systems approach will support effective capacity building efforts, as well as how it integrates with existing cybersecurity capacity building processes. Included showing how applying tools and stakeholder analysis and breaking down the systems concept might work and the potential benefits of the systems concept to cybersecurity education capacity building.

Findings reinforce the notion that national cybersecurity education capacity building is a complex system composed of many interacting components that exist in a dynamic environment. In response, capacity building actions must reflect this complexity and develop holistic and multi-stakeholder solutions to find targeted and sustainable ways to improve national cybersecurity education capacity and create a resilient cybersecurity workforce and society.

Based on these conclusions, the following recommendations and next steps are intended for countries to consider as part of their own national cybersecurity education capacity building efforts.

• Develop a national cybersecurity capacity systems concept: map the existing environment, identify current capacity building actions, and identify gaps and opportunities to strengthen and expand these activities.

• Complete a national cybersecurity education capacity maturity assessment: map current capacity and establish a baseline or benchmark against which progress in future national capacity building efforts can be measured.

• Explore a wide range of relevant systems thinking tools to develop a national cybersecurity capacity systems concept: define national challenges and opportunities for capacity building.

• Consider the absorption capacity of the national cybersecurity education system when designing a capacity building programme: integrate any new measures both in terms of volume and type.

• Consider how cybersecurity capacity building integrates with the broader national development context and priorities.

• Collate existing and new research to support the analysis of national cybersecurity capacity environment.

• Support bilateral and multilateral knowledge exchange to share lessons learnt from national cybersecurity education in different geographical and development contexts.

• Encourage knowledge exchange and cooperation between governments, private sector, and civil society stakeholders.

• Share successful approaches to reduce duplication of effort and increase economies of scale.

• Consider the three levels of capacity (individual, organisational, and enabling environment) and how these will be addressed as part of the intervention design, implementation, and evaluation. When designing capacity building for primary school

students, for example, the individual might be the primary school students or teachers, the organisation might be the schools, and the enabling environment might be the education policy and system in each country.

There is a broad range of actions that countries can pursue to support national cybersecurity education capacity building efforts having completed their mapping exercise as recommended above. These include short-to-medium term measures that rapidly improve capacity and mitigate risk and threats. In addition, Member States should also consider medium- to long-term measures that focus on building a more sustainable and resilient approach.

Short- to medium-term measures:

• Create cyber career conversion programmes focused on professions with translatable skill sets that can easily transition into cybersecurity roles.

• Support train-the-trainer initiatives to build a cadre of cybersecurity trainers.

• Build targeted talent programmes e.g., focused at increasing the participation of women in the cybersecurity workforce.

• Transfer and adopt existing successful training and courses and best practice.

• Ensure support for underrepresented groups such as women in cyber fellowship programmes.

• Ensure grassroots support such as cybersecurity apprenticeship programmes.

• Promote cybersecurity hiring practices that focus on core requirements and avoid unnecessary barriers to entry.

• Support and expand on-the-job cybersecurity training and employee development.

Medium- to long-term measures:

• Develop a national cybersecurity education strategy to outline a holistic approach and communicate priority areas and goals.

• Analyse strategic drivers that will reflect the need for specific cybersecurity skills to reach national digital development goals and mitigate against anticipated cybersecurity risks and threats.

• Developing a national cybersecurity workforce framework to create a common reference point and taxonomy for supply and demand side stakeholders.

• Develop a training needs assessment strategy to determine cybersecurity roles, proficiency levels and volume required to upskill the workforce.

• Design a national learning model, as well as training development pathways to determine the cybersecurity curriculum, certification process, and learning preferences that can most efficiently build a scalable and quality assured national model.

• Run targeted initiatives at primary and secondary schools aimed at building the relevant knowledge, skills, and interest for a career in cybersecurity.

• Run targeted initiatives to build awareness, knowledge, and skills of priority groups to effectively contribute to a cybersecure workforce and cybersecure society.

• Runn executive level initiatives focused to promote leadership and buy-in to the importance of cybersecurity.

• Invest in national cybersecurity research and development that will improve education and training.

• Develop an interactive dashboard to provide actionable data on supply and demand in the cybersecurity job [41].

The next steps and areas for future work to support Member States to further their cybersecurity capacity building include:

1. Reaching out to members of the global cybersecurity capacity building community to collect feedback on the application and benefits of the systems concept and approach to national cybersecurity capacity building.

2. Working with low- and middle-income economies to utilize systems thinking concepts as a basis for the development of national cybersecurity education frameworks.

3. Continuing with regular reviews of cybersecurity education capacity building research, incorporating a broad range of sources and perspectives with potential focus areas including:

• how to engage with underrepresented communities and groups such as women, older people, and people with disabilities;

• how to feature and prioritize cybersecurity education in existing national cybersecurity strategies;

• how to ensure sustainable capacity building.

4. Refining, testing, and validation of the cybersecurity capacity systems concept through research in relevant cybersecurity education contexts including expert interviews, surveys, and focus groups, with particular consideration to:

• key stakeholders;
• success indicators for capacity building;
• system component relationships;
• system leverage points; and
• future applications to a variety of national contexts (e.g., different levels of income, population size and distribution, technology adoption and reliance, as well as systems of government and other relevant factors).

5. Exploring the use and integration of other systems thinking tools in relation to national cybersecurity education capacity building.

6. Considering how to convert this study and future research into a guide for Member States to develop a national cybersecurity education and training capacity building strategy.

7. Developing a toolkit that includes templates and guidance notes to support Member States to apply the systems concept.

8. Exploring the development of an interactive digital dashboard resource that can be customed to assist Member States to map a national cybersecurity education capacity system and linkages, and track changes over time.

This framework, designed to help countries understand and navigate their unique cybersecurity ecosystems, emerged from the recognition of the need for a more comprehensive approach to cybersecurity capacity development [42-43]. By fostering a deeper understanding of the cybersecurity education ecosystem, this approach aims to balance immediate workforce gaps with long-term requirements, ensuring sustained cybersecurity resilience.

REFERENCES

[1] World Economic Forum. Global Cybersecurity Outlook 2022. Insight Report. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

[2] (ISC2) Cybersecurity Workforce Study 2022 https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf

[3] United Nations. SDG 4 Quality Education. 2023. https://sdgs.un.org/goals/goal4

[4] UNICEF. Digital Literacy in Education Systems Across ASEAN. 2021. https://www.unicef.org/eap/media/7766/file/Digital%20Literacy%20in%20Education%20Systems%20Across%20ASEAN%20Cover.pdf

[5] Vladimir Radunovic, David Rüfenacht, "Report on cybersecurity competence building trends in OECD countries," 2016. https://www.diplomacy.edu/resources/general/cybersecurity-competence-building-trends

[6] Pavlov S.V., Dokuchaev V.A., Maklachkova V.V., Gadasin D.D. (2023) Automated Decision Support for Selection of Specialists for Complex Infocommunication Systems Management. T-Comm, vol. 17, no. 12, pp. 36-43. DOI: 10.36724/2072-8735-2023-17-12-36-43.

[7] Statev V.Yu., Dokuchaev V.A., Maklachkova V.V. (2022) Information security in the big data space. T-Comm, vol. 16, no.4, pp. 21-28. DOI: 10.36724/2072-8735-2022-16-4-21-28.

[8] Aspen Cybersecurity Group. Principles for Growing and Sustaining the Nation's Cybersecurity Workforce. 2018. https://www.aspeninstitute.org/wp-content/uploads/2018/11/Aspen-Cybersecurity-Group-Principles-for-Growing-and-Sustaining-the-Nations-Cybersecurity-Workforce-1.pdf.

[9] De Zan, Di Franco, "Cybersecurity Skills Development in the EU," 2019. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union.

[10] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, K.K.R. Choo, "The role of national cybersecurity strategies on the improvement of cybersecurity education," *Computers & Security*, 2022, p. 119.

[11] S. Creese, W. H. Dutton, P. Esteve-González, "The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions," *Personal and ubiquitous computing*, 2021, no. 25(5), pp. 941-955. https://doi.org/10.1007/s00779-021-01569-6

[12] F. E. Catota, M. G. Morgan, D. C. Sicker, "Cybersecurity education in a developing nation: The Ecuadorian environment," *Journal of Cybersecurity*, 2019, no. 5(1).

[13] GFCE Working Group D. Developing Cyber Security as a Profession. 2022. https://thegfce.org/wp-content/uploads/2022/08/GFCE-Report-Developing-Cyber-Security-as-a-Profession-July-2022-1.pdf.

[14] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, F. Khalid, "The importance of cybersecurity education in school," *International Journal of Information and Education Technology*, 2020, no. 10(5), pp. 378-382.

[15] B. J. Blazic, "Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?" *Educ Inf Technol,* 2022, no. 27, pp. 3011–3036. https://doi.org/10.1007/s10639-021-10704-y.

[16] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta and R. De Nicola, "Framework, Tools and Good Practices for Cybersecurity Curricula," *IEEE Access*, 2021, vol. 9, pp. 94723-94747. https://doi.org/10.1109/ACCESS.2021.3093952

[17] R. Shillair, P. Esteve-González, W. H. Dutton, S. Creese, E. Nagyfejeo, B. von Solms, "Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise," *Computers & Security*, 2022, no. 119, https://doi.org/10.1016/j.cose.2022.102756.

[18] ITU. Global Cybersecurity Index (GCI). 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[19] E-Governance Academy Foundation. National Cyber Security Index (NCSI). 2020. https://ncsi.ega.ee/
[20] ENISA. National Capabilities Assessment Framework (NCAF). 2020. https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework
[21] Global Cyber Security Capacity Centre. Cybersecurity capacity maturity model for nations (CMM): Revised edition. 2021. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf
[22] Potomac Institute. (Cyber Readiness Index (CRI) 2.0. 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf
[23] Dokuchaev V.A., Maklachkova V.V., Statev V. Yu. (2020) Digitalization of the personal data subject. T-Comm, vol. 14, no.6, pp. 27-32. DOI: 10.36724/2072-8735-2020-14-6-27-32.
[24] Pavlov S.V., Dokuchaev V.A., Maklachkova V.V., Mytenkov S.S. (2019). Features of supporting decision making in modern enterprise infocommunication systems. T-Comm, vol. 13, no.3, pp. 71-74. DOI 10.24411/2072-8735-2018-10252.
[25] L. Bate, “Cybersecurity Workforce Development: A Primer. New America, Florida International University,” 2018. https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_Workforce_Development_A_Primer_2018-11-01_183611.pdf
[26] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, A. Josang, E. Stavrou, “Global perspectives on cybersecurity education for 2030: a case for a meta-discipline,” *Procedings companion of the 23rd annual ACM conference on innovation and technology in computer science education*, 2018, pp. 36-54.
[27] OAS. Cybersecurity Education. 2020. https://www.oas.org/es/sms/cicte/docs/White-Paper-Cybersecurity-Education.pdf
[28] Henry, Adam P., “Mastering the Cyber Security Skills Crisis: Realigning Educational Outcomes to Industry Requirements,” 2017. https://unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/ACCS-Discussion-Paper-4-Web.pdf
[29] J. Bridge, J. Twaddle, “Scaling up work integrated learning in higher education,” 2023. https://www.pwc.com.au/government/government-matters/work-integrated-learning-in-higher-education.html
[30] Western Sydney University. Industry Placement Pathway. 2023. https://online.westernsydney.edu.au/online-courses/social-science/bachelor-cyber-security-behaviour/placement-pathway/
[31] Guide to Developing a National Cybersecurity Strategy. GFCE Working Group D. White Paper: Task Force on Cybersecurity Professional Training and Development. 2019. https://cybilportal.org/wp-content/uploads/2020/02/GFCE-WG-D-White-Paper-Task-Force-on-Cybersecurity-Professional-Training-and-Development.pdf.
[32] W. Newhouse, S. Keith, B. Scribner, G. Witte, “National initiative for cybersecurity education (NICE) cybersecurity workforce framework,” *NIST special publication*, 800(2017), 181.
[33] European Commission. Operational Guidance for the EU’s international cooperation on cyber capacity building. 2018. https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building
[34] Allen & Kilvington. Summary: An introduction to systems thinking and systemic design – concepts and tools (Presentation). Based on material for an introductory workshop. 2018. https://learningforsustainability.net/post/systemicdesign-intro/
[35] OECD. Systems Approaches to Public Sector Challenges. 2017. https://www.oecd.org/publications/systems-approaches-to-public-sector-challenges-9789264279865-en.htm
[36] Learning for Sustainability. Systems Thinking. 2020. https://learningforsustainability.net/systems-thinking/
[376] Social Value International. Maximise Your Impact: A guide for social entrepreneurs. 2017. https://socialvalueint.org/maximise-your-impact-guide
[38] REWIRE Project. PESTLE analysis of Cybersecurity Education. 2021. https://digital-skills-jobs.europa.eu/en/inspiration/research/pestle-analysis-cybersecurity-education-2021
[39] I. Agrafiotis, M. Bada, P. Cornish, S. Creese, M. Goldsmith, E. Ignatuschtschenko, D. M. Upton, “Cyber harm: concepts, taxonomy and measurement. Saïd Business School WP,” 2016.
[40] Stakeholder Mapping Adapted from: Social Value UK. Maximise Your Impact – A Guide for Social Entrepreneurs. 2017. http://www.socialvalueuk.org/app/uploads/2017/10/MaximiseYourImpact.24.10.17.pdf
[41] Interactive dashboard for the United States of America: Cyber Seek. 2023. https://www.cyberseek.org/
[42] A systems approach to understanding national cybersecurity education capacity. 2024. https://www.itu.int/hub/publication/d-phcb-cyb_educ-2024/
[43] Dokuchaev V.A., Maklachkova V.V., Statev V.Yu. (2020) Classification of personal data security threats in information systems. *T-Comm*, vol. 14, no.1, pp. 56-60. DOI: 10.36724/2072-8735-2020-14-1-56-60.