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

JOURNAL OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGIES

СПИСАНИЕ ЗА ЕЛЕКТРОТЕХНИКА И ИНФОРМАЦИСКИ ТЕХНОЛОГИИ

J. Electr. Eng. Inf.. Technol.	Vol.	No.	pp.	Skopje
	7	2	63–114	2022
Спис. Електротехн. Инф. Технол.	Год.	Број	стр.	Скопје

J. Electr. Eng. Inf.. Technol.	Vol.	No.	pp.	Skopje
	7	2	63–114	2022
Спис. Електротехн. Инф. Технол.	Год.	Број	стр.	Скопје

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

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

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

Published twice yearly – Излегува два пати годишно

INTERNATIONAL EDITORIAL BOARD – МЕЃУНАРОДЕН УРЕДУВАЧКИ ОДБОР

Liljana Gavrilovska, Ss Cyril and Methodius University in Skopje, **Alberto Leon Garcia**, University of Toronto, Canada, **Goga Cvetkovski**, Ss Cyril and Methodius University in Skopje, **Damir Žarko**, University of Zagreb, Croatia, **Atanas Iliev**, Ss Cyril and Methodius University in Skopje, **Marko Čepin**, University of Ljubljana, Slovenia, **Hristina Spasevska**, Ss Cyril and Methodius University in Skopje, **Rubin Taleski**, Ss Cyril and Methodius University in Skopje, **Miomir Kostić**, University of Belgrade, Serbia, **Gjorgji Dimirovski**, Dogus University, Turkey, **Zoran Ivanovski**, Ss Cyril and Methodius University in Skopje, **Dragica Vasilevska**, Arizona State University, USA, **Aristotel Tentov**, Ss Cyril and Methodius University in Skopje, **Dragan Denić**, University of Niš, Serbia, **Aleksandar Dimitrovski**, University of Central Florida, USA, **Marjan Popov**, Delft University, The Netherlands, **Snežana Čundeva**, Ss Cyril and Methodius University in Skopje, **Lothar Fickert**, University of Graz, Austria, **Đani Juričić**, Institute Jožef Šefan, Slovenia, **Lina Karan,** Arizona State University, USA, **Khalil El Khamlichi Drissi**, University of Clermont Auvergne, France, **Oleh Velychko,** Ukrmetrteststandart, Kiev, Ukraine

Editor in Chief **Acad. Leonid Grčev**	Одговорен уредник **Акад. Леонид Грчев**
Co-editors in Chief **Dimitar Taškovski, Mile Stankovski, Vladimir Dimčev, Aleksandar Risteski**	Заменици одговорни уредници **Димитар Ташковски, Миле Станковски, Владимир Димчев. Александар Ристески**
Secretary **Mare Srbinovska**	Секретар **Маре Србиновска**
Graphics and art design **Blagoja Bogatinoski**	Графичко и ликовно обликување **Благоја Богатиноски**
Proof-reader **Alena Georgievska**	Коректор **Алена Георгиевска**

UDC: "St. Kliment Ohridski" Library – Skopje	УДК: НУБ „Св.. Климент Охридски" – Скопје
Copies: 300	Тираж: 300
Price: 760 denars	Цена: 760 денари
Address	Адреса

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

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

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

J. Electr. Eng. Inf.. Technol.	Vol.	No.	pp.	Skopje
	7	2	63–114	2022
Спис. Електротехн. Инф. Технол.	Год.	Број	стр.	Скопје

TABLE OF CONTENTS
(С О Д Р Ж И Н А)

Telecommunications – Телекомуникации

Automatics – Автоматика

Electronics – Електроника

Metrology – Метрологија

Journal of Electrical Engineering and Information Technologies, Vol. **7,** No. 2, pp. 67–75 (2022)
Article 197
Received: Octomber 10, 2022
Accepted: November 11, 2022
In print: ISSN 2545–4250
On line: ISSN 2545–4269
UDC: 004.7.056:004.416'2
DOI: https://doi.org/10.51466/JEEIT2272197067g

Original scientific paper

ANALYSIS AND DESIGN OF SECURITY SOLUTIONS IN INTERNET NETWORK

Filip Gligorov, Toni Janevski

Faculty of Electrical Engineering and Information Technologies,
"Ss. Cyril and Methodius" University in Skopje,
Rugjer Bošković bb, P.O. Box 574, 1001 Skopje, Republic of North Macedonia
tonij@feit.uki.edu.mk

A b s t r a c t: The birthday of the Internet is considered January 1, 1983, by standardizing the IP and TCP. Even though its use and purpose have changed over time, one of the main challenges has been constantly present throughout the years, and that is security. Security in the Internet network includes all activities that individual users, organizations, enterprises, and institutions undertake to protect their value as well as the integrity and continuity of operations in telecommunication networks and systems. Besides the development of tools and mechanisms for enabling a safe and secure network, there is a parallel "development" of tools and mechanisms for breaking into those security systems. This paper analyzes the various scenarios and possible threats and attacks on the Internet and in general on IP-based networks and provides an overview of network security design with the implementation of system solutions.

Key words;; security analysis; security attacks; threats; vulnerabilities; intrusion

АНАЛИЗА И ДИЗАЈН НА РЕШЕНИЈА ЗА БЕЗБЕДНОСТ ВО ИНТЕРНЕТ-МРЕЖАТА

А п с т р а к т: Појавата на Интернетот во форма која денес се користи датира од 1983 година, со стандардизацијата на IP и TCP. Иако неговата употреба и намена се имаат променето со текот на времето, сепак еден од главните предизвици низ годините е постојано присутен, а тоа е безбедноста. Безбедноста во Интернет-мрежата ги вклучува сите активности што индивидуалните корисници, организациите, претпријатијата и институциите ги преземаат за да ја заштитат својата вредност, како и интегритетот и континуитетот на операциите во телекомуникациските мрежи и системи. Всушност, со развојот на алатки и механизми за овозможување безбедна и сигурна мрежа паралелно се одвива и „развивањето" на алатки и механизми за пробивање на тие безбедносни системи. Овој труд ги анализира различните сценарија и можни закани и напади на Интернет и, генерално, на мрежте базирани на IP, и дава осврт на дизајн на безбедност за мрежата со имплементација на системски решенија.

Клучни зборови: безбедносна анализа; безбедносни напади; закани, пропусти; упад

1. INTRODUCTION

"In this age of universal electronic connectivity when the world is becoming a global village, different threats like viruses and hackers, eavesdropping and fraud, undeniably there is no time at which security does not matter.

Volatile growth in telecommunication systems and networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This leads to a sharp awareness of the need to protect data and resources to disclosure, to guarantee the authenticity of data and messages, and protection of systems from network-based attacks." [1]

Securing a telecommunication network is a complicated job. Different levels of security are appropriate for different organizations. Organizations and individuals can ensure better security by using a systematic approach that includes analysis, design, implementation and maintenance. The analysis phase requires that you thoroughly investigate

your entire network, both software and hardware, from inside and outside. This helps to establish if there are any vulnerabilities. The analysis shows what is in place today and what you may require for tomorrow [2].

The main focus of this paper is to come up with a better understanding of network security applications and standards. To achieve these goals, the following parameters have been investigated:

- security threats and vulnerabilities,
- security attacks,
- security techniques and tools,
- security solutions.

This paper is organized based on the aforementioned arguments. The second section presents an overview of the most common weaknesses and vulnerabilities in a telecommunication network. Section 3 covers the possible attacks that can be executed on a network, and the next section, section 4, explains the techniques and tools that can prevent and secure the network from attackers. Lastly, section 5 gives the mechanisms for implementing security solutions.

2. SECURITY THREATS AND VULNERABILITIES

Network security is the protection of networks, their applications or services against unauthorized access that prevents modification, disclosure or destruction of data. It also assures that the network is performing correctly with no harmful side effects [3]. Each organization defines its security policy that describes the level of access, which is permitted or denied. So any organization must make such a security mechanism that is broad in scope and helps to deal with new types of attacks.

Vulnerabilities are defined as weaknesses in any network that can be exploited by a threat. One telecommunication network consists of different network devices, appliances, computers, as well as applications running onto the mentioned hardware. Protecting these bits and pieces of the telecommunication network is the most important task in the process of making a secured telecommunication environment. There are different hardware and software tools that can contribute to protecting the network from attacks, such as firewalls, Intrusion Detection Systems (IDS), antivirus software and vulnerability scanning software. Following are some of the common threats to the network.

One of the main advantages of any network is the ability to share resources. As a part of a network, different types of services can be shared, like file and printer sharing. Gaining illegal access to these resources causes unauthorized access in the network. Password sharing, guessing and capturing are the most common methods to gain illegal access. Password sharing and guessing can be achieved using different techniques like:

- Try default passwords.
- Try dictionary words.
- Try short words (1–3 characters long).
- Try the user's personal number, home address, and personal information like birth date, family name, etc.

Password capturing is a technique in which a hacker unknowingly steals a user's ID and password. The Trojan horse program is specifically designed for this purpose. Below is some recommended information that can prevent unauthorized access:

- Use strong passwords, at least 10 characters long, containing letters, numbers and special characters and avoid using dictionary words.
- Use hardware and software firewalls.
- Use protection software.

Companies have different departments and users, some users may have inappropriate access to network resources, mostly because the users are not from the same department or may be such users who are from outside the company. Moreover, information stored in the network may require a level of confidentiality. Illegal access occurs when someone who is not authorized tries to read that data.

So far mentioned threats can be classified as compromising data that reside in a system or computer. The second type of data breach is while transferring from machine to machine or while sharing among the network users. These two types of data fall under two types of security, computer and network security. The tools that are designed to protect the first type of data fall under computer security while the protection of data during transmission is called network security. During the transmission of data two things are important that assure the integrity of data, one is that data is coming from a trusted host and the second is that data contents are not altered or changed. Spoofing occurs when someone pretends to be a trusted host. IP spoofing, Email spoofing, Web spoofing, etc, are some types of spoofing. Messages transmitted over any network

consist of some address information, sender address and receiver address. An intruder or hacker who initially finds the IP address of a trusted host after compromising the host can modify the message (packet header) so that it appears that the message is coming from that trusted host [3], as shown in Figure 1.

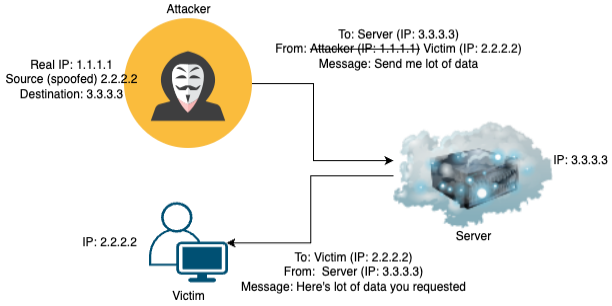


Fig. 1. IP spoofing

When a network does not provide the needed functionality on time means that a disruption has occurred. Several reasons may lay behind that: the network cannot detect the traffic, it has a single point of failure, it has a hardware failure, improper maintenance of network equipment, etc. Knowing all these threats and vulnerabilities in a telecommunication network, the implementation of a security mechanism sometimes cost too much, therefore some administrators simply tolerate the expected losses and find the most cost-effective solution.

3. NETWORK SECURITY ATTACKS

The way of locking down an "open" system to avoid its usage by anyone represents the security of that system. Any action that compromises security is called a security attack. A system which is providing the services required by the user accurately and preventing the illegal use of system resources is called a secure system. Attacks can be categorized into following basic categories [4]:

- Interruption: For using the data or resources they must be available 24/7 for the authorized parties, when and where they need it. An attack on the availability of data is called interruption. Availability can be affected by intentional or unintentional acts. Unintentional acts are, accidental system crashes, deletion and overwriting of data and sometimes due to non-human factors like floods, fires and earthquakes. Examples of intentional acts are attacks by hackers that crash the system, such as denial of service (DOS) and distributed denial of service (DDOS) attacks.
- Interception: The core concept is that the data should be hidden from unauthorized users. If someone who is unauthorized sees or copies the data then that data can be used in an intensive active attack. Such an attack is known as an attack on confidentiality.
- Modification: The integrity of data deals with the prevention of intentional or unintentional modification of data. An attack on the integrity of data is called a modification. Protection of data from modification is a foremost concern than detection.
- Fabrication: An attack on authenticity is called fabrication. Authenticity means that message is coming from the apparent source.

Above mentioned attacks are shown in Figure 2. Based on these four attacks, we can further classify security attacks as passive and active attacks. Passive attacks are only involved in the monitoring of the information (interception). The goal of this attack is to obtain transmitted information. Passive attacks are hard to detect because they do not involve in alteration. Active attacks are involved in the modification of data (interception, modification, fabrication) or the creation of false data. The information which hackers obtained from a passive attack is used in a more aggressive active attack [5–7].

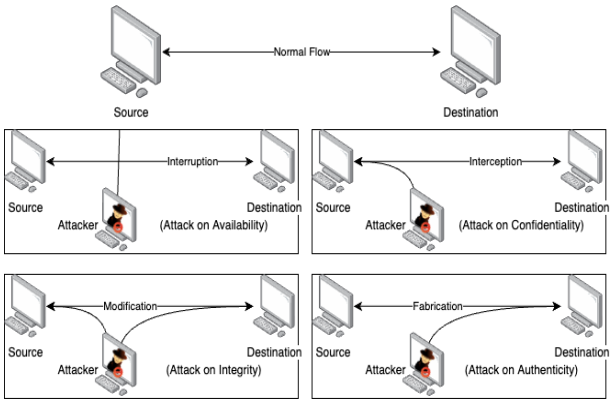


Fig. 2. Types of security attacks

Gathering information against a targeted host or network is called a reconnaissance attack. Attacker analyzes the target host and tries to discover details like live IP addresses, open ports of the network, failure of an operating system, and types of

services and protocols running on the network. Reconnaissance attacks are common, they are not so dangerous because they are not involved in any kind of alteration or destruction of data but, on the other hand, they show the vulnerabilities in the network. Following is presented some of the reconnaissance attacks (packet sniffing, port scan/ping sweep and Internet information queries).

A packet sniffer is a tool or device that can be used for capturing the packet at the data link layer. A packet sniffer is not only a hacker's tool but it can be used both by the hacker for eavesdropping and by the administrators for network monitoring and troubleshooting. Tcpdump, Windump, Wireshark (ethereal) and Dsiniff are examples of different sniffing tools. Sniffing can be passive or active.

When using hubs in the network, each machine in that network decides whether to accept or discard the broadcasted packet. In passive sniffing, this filter in the machine is disabled, thus the machine can capture the traffic and then analyze the content of the packages [8, 10]. Figure 3 shows the passive sniffing.

In a network where switches are used, the packages are directed from the source to the destination machine. In such a case, an active sniffing mechanism takes over, like MAC Flooding and Spoofed ARP Messages. Switches worked based on MAC addresses. They maintain an ARP table in a special type of memory called Content Addressable Memory (CAM). ARP table has all the information of which IP address is mapped on which MAC address. The act of overloading the CAM is known as MAC flooding. At this stage, the switch goes to a fail-open mode [9, 10] and cannot perform IP to MAC mappings, starts behaving like a hub, and starts transmitting the data to all machines.

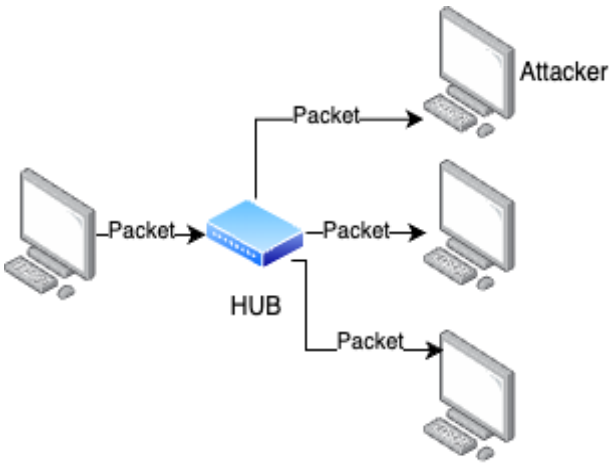


Fig. 3. Passive sniffing

In the active sniffing technique, spoofed ARM messages, the attacker tries to be the destination machine. Poisoning the ARP cache of a central entity of the network, the attacker maps his MAC address to the IP address of the switch (or router). In this way, all the traffic first goes towards the attacker and then the router [11]. Active sniffing is shown in Figure 4.

Port scan and ping sweep are two common network probes typically used to run various tests against a host or device to find vulnerable services. They are helpful to examine the IP address and the services which are running on a device or host. In port scanning, a packet is sent to each target port and the reply message indicates that either the port is open or closed which is further helpful to launch an attack against a specific service [12].

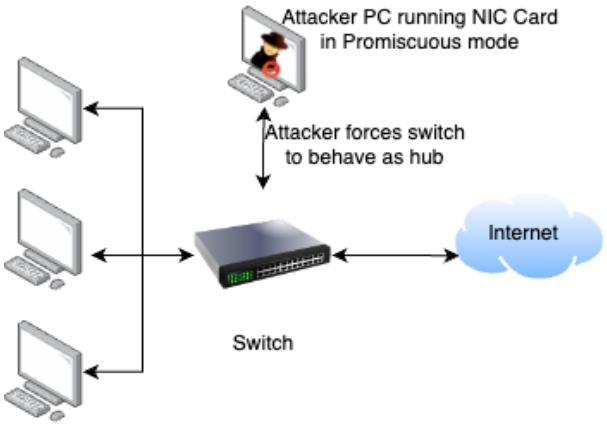


Fig. 4. Active sniffing

The most popular probing tool is Nmap. The method of finding which IP addresses are live is called ping sweep. The aim is to find out machines which are alive and which are not alive. These ICMP replies from different machines are logged into a file for future reference. Fping is a tool used for performing ping sweep. Working on the round robin function, it takes a list of IP addresses, sends a ping packet to an IP address, and immediately proceeds toward the next IP address.

The reconnaissance attacks are completed with internet information queries. DNS queries provide the particular information of the domain and the addresses associated with that particular domain. IP queries display the range of IP addresses and for which domain those addresses are associated. Ping sweep presents a clear picture of a particular environment. After these queries port scan starts by the hacker which leads him to find out which ports are

open and which services are running on these ports. Finally, the whole information can be helpful when a hacker tries to compromise any system through these services.

Other than the reconnaissance attacks, there are also access attacks. Access attacks occur when a hacker exploits the vulnerabilities of the services running on a system and succeeds to access confidential information. Different types of network attacks are password attacks, trust exploitation, port redirection, and man-in-the-middle attack.

Several methods can be used for password attacks. Trojan horse, IP spoofing and packet sniffers can show the detail of the user like user name and password. The password attack can be referred to as repeated attempts to find the user information (user name or password). Once an intruder succeeds then he/she has the same access right that the compromised account has. In Table 1, the different type of password cracking attacks are presented.

Table 1

Type of password attacks

	Dictionary attack	Brute force attack	Hybrid attack
Speed of the attack	Fast	Slow	Medium
Passwords cracked	Finds only words	Finds every password (A–-Z, 0–9, special characters)	Finds only the passwords that have dictionary word as the base

When a hacker attacks – a computer that is outside a firewall and that computer has a trust relationship with another computer that is inside the firewall, the hacker can exploit this trust relationship. Figure 5 explains trust exploitation.

The port redirection is another type of trust exploitation attack in which a hacker bypasses the security mechanism. Figure 6 shows the port redirection attack.

When hackers succeed to intrude between two communication parties this type of attack is called a MITM (Man-in-the-Middle) attack. In this way hackers can intercept data between source and destination host, can modify data and retransmit it to the destination host, and can also inject any type of false data. MITM attacks can affect on availability, confidentiality, integrity, and authenticity of data.

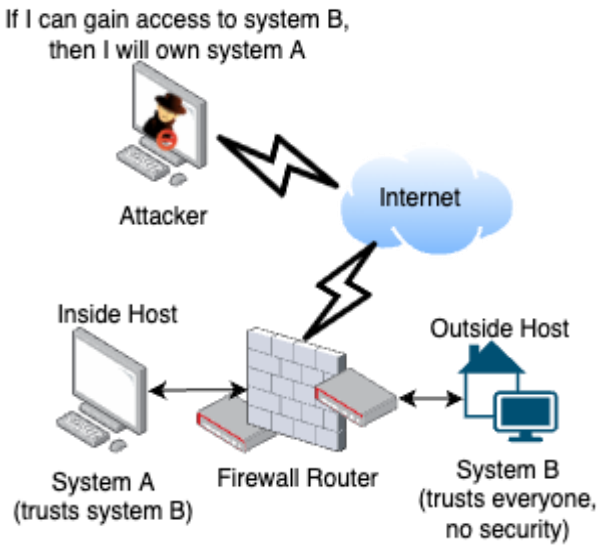


Fig. 5. Trust exploitation attack

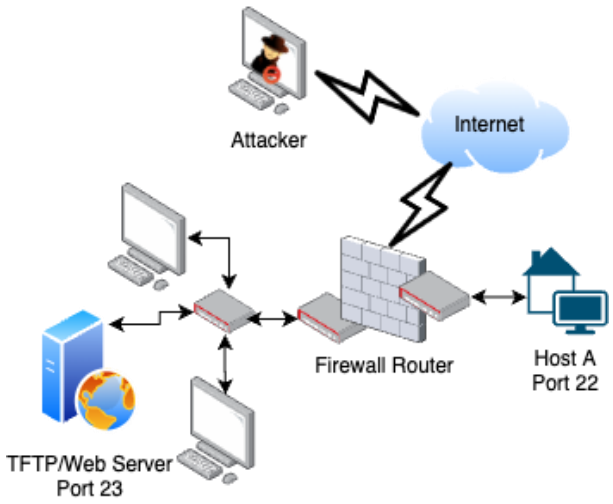


Fig. 6. Port redirection attack

Types of attacks that bring the network down in such a way that resources are not available even for authenticated users are known as DOS attacks. Attackers may target a single machine to make it impossible for outgoing connections on the network or may attack the whole network to make it impossible for incoming and outgoing traffic. Ping of death, SSPing, Land, Win Nuke, and SYN flood are some examples of DOS attacks. In an SYN flood attack, a hacker sends an SYN packet to a target host which then responds with SYN acknowledgment, at the end attacker does not send any ACK packet to the target host which causes the connection to remain in a half-open state. TCP connection does not remove this connection from its table and wait to expire this session, the attacker takes the

advantage of this and continues sending new SYN packets until the TCP SYN queue is filled and cannot accept new connections [13].

4. SECURITY COUNTERMEASURE TECHNIQUES AND TOOLS

The security countermeasure techniques are directly related to such parameters that survive in the form of network bugs or vulnerabilities and their effects on a communication network. After analyzing the effect of these parameters, appropriate security countermeasure techniques for the network can be selected.

The selection and implementation of these countermeasure techniques in a network environment depend on the network administration team. It depends upon their updated knowledge and awareness about the network, standard network architecture, traffic parameters in the form of application behavior (OSI and TCP/IP layer network protocols knowledge and working role), network hardware performance, security threats, and existing weak points in the network. A rough or out-of-date knowledge can become a cause of network bugs and vulnerabilities.

By considering the above measurements many research organizations have assigned some most essential key security countermeasure techniques for a standard-level network infrastructure [14].

A strong security policy performs an efficient role in a network. If policy develops after analyzing the network and behavior of its components then it results in a much more secure and smooth network.

The authorization of systems or network resources has an important role in security countermeasures. After a fair survey of the network, a proper level of authority for accessing the system resources can be assigned. The policies of antivirus or the access control list of routers or firewalls can define the authority for properly accessing network resources.

The presence of an intrusion detection system has an important role in security countermeasures. The study and analyzing the log files against malicious activities in the network can save a system. It provides a futuristic safety approach against many other malicious aims.

The symptoms of a malicious attack give us an idea about which type of protection is required for a system against that attack. We can re-adjust or reconfigure our security system parameters by generating a strong resistive block against the attack.

By fixing basic problems in a system or network we can save the system or network. These basic but core problems are hidden spot that exists in any common network or system, like improper updating of system applications, out-of-date applications, and updated virus patches (not on proper time) these all can create a security flaw in any network [15].

As a complement to countermeasure techniques are the countermeasure tools, such as cryptography, conventional or symmetric encryption, and public key or asymmetric encryption.

Cryptography is used to protect data from interception. It is the study of methods to send data in unrecognizable form so that only the intended user can recognize and read the message. Cryptography concerns with two things, data is coming from an apparent or trusted source and the contents of data are not altered. Goals that can be achieved from cryptography are confidentiality, data integrity, authentication, and non-repudiation.

Conventional or symmetric encryption has been the only encryption scheme available before public-key encryption. One secret key is shared among the sender and the receiver. The whole procedure of conventional encryption consists of five stages:

1. Plain text: The original message or data that needs to be encrypted.
2. Encryption algorithm: The encryption algorithm performs different transformations on the data.
3. Secret key: Secret key is the input to the encryption algorithm. Different transformations performed by the encryption algorithms depend on the secret key.
4. Cipher text: This is the output of a scrambled message.
5. Decryption algorithm: Reverse the encryption algorithm, and produces the plain text with the help of the same secret key and the cipher text.

One important thing is that the security of conventional encryption depends on the secret key, not on the algorithms. Even if the cipher text and algorithms are known, it is practically impossible that a message can be decrypted with the help of cipher text and encryption/decryption algorithm. In most symmetric algorithms two communication parties use the same key for encryption and decryption which is why it is also called a secret-key, single-

key, or one-key algorithm. For safe communication, the key must remain secret. It is also necessary to change the key frequently so that attacker could not compromise the key. The strength of any cryptographic system depends on the key distribution process. There are several ways to distribute the keys between two parties A and B [16].

- Key could be selected by party A and physically delivered to party B.
- Any third party could select a key and physically deliver it to A and B.
- If A & B have previously used a recent key, one party could transmit the new key to the other, which is encrypted by the old key.
- In case of encrypted connection of A & B to a third party C, the third party C could deliver the key to A & B on encrypted links.

Instead of using one key which is used in conventional encryption, asymmetric uses two separate keys. The use of two keys makes communication more secure and authenticated. The asymmetric scheme has six ingredients:

1. Plain text: The original message or data.
2. Encryption algorithms: The encryption algorithm performs different transformations on the data.
3. Public and private key. The transformation by the encryption algorithm totally depends on these keys. These keys are selected in such a way that if one is used for encryption, the other is used for decryption.
4. Cipher text: This is the output scrambled message.
5. Decryption algorithm: Reverse the encryption algorithm.

Public and private keys are used in public-key encryption, as name suggests that public key is used publicly while private key is only used by its owner. The following steps are followed in public-key encryption:

1. Each and every user in a network generate a pair of keys, one is used for encrypting the message while other is for decrypting the message.
2. From those two keys each user places one key in a public register, so that every other user can access that key. In this way each user has a collection of public keys of all the users in network.
3. If user A wants to send a message to user B, A encrypts a message with B's public key.
4. When user B receives the message, he/she decrypts it by using his/her private key. No one else can decrypt this message.

The major weakness in public-key encryption is that public key is public. Thus, anyone can forge such type of public announcement. An intruder could pretend to be user A and can send its public key to any other participant or even can broadcast his public key. The solution is to use public-key certificate issued by a third party which is called Certificate Authority (CA). This authority is trusted by the user community it can be any governmental organization that issues a certificate which consists of public key, user ID of the key owner and at the end whole block is signed by the CA. X.509 is a standard scheme used in most network security applications for certification [17].

5. SECURITY SOLUTIONS

Once the network threats and vulnerabilities are known as well as the techniques for establishing the secure network, the next step is implementing solutions that make the telecommunication network reliable and protected. Depending on their implementation, security solutions mainly can be categorized as application-level solutions and system-level solutions.

Application security solutions start with the authentication. The verification of any identity is called authentication which also verifies the integrity of the data. For the telecommunication networks, Kerberos and X.509 are used to keep the data integrity.

In traditional networks, a user types a password to verify his identity, this is called authentication. Password-based authentication is not a good solution because passwords are sent across the network and any intruder can intercept these passwords. Strong authentication-based cryptography is required so that intruders could not gain information that will help to impersonate him. The most common example of this type of authentication is Kerberos, which is based on conventional encryption. It is a distributed authentication service in which the server verifies a user without sending information on the network [18].

X.509 is another authentication protocol based on a public-key certificate. The authentication protocols defined in X.509 are widely used, for example in S/MIME, IP Security, and in SET. The Certificate consists of a public key of the user, signed by the private key of that trusted party and that party is called Certificate Authority (CA).

The most widely used and growing network application across all platforms is electronic mail. To keep the confidentiality of e-mail two schemes are used, PGP and S/MIME.

Pretty Good Privacy (PGP) combines the features of the two cryptographic schemes. First, it compresses the message and then creates a one-time secret key for data encryption, this key is called a session key. The data is encrypted with this one-time session key and the session key is also encrypted by the recipient's public key. This encrypted session key and cipher text then are transmitted to the recipient. On the recipient's side, PGP recovers that session key with the help of a private key and this recovered session key then is used to decrypt the cipher text.

Secure/Multipurpose Internet Mail Extension (S/MIME) provides security for MIME data by signing the data and by use of public-key encryption. It provides authentication of data by using a digital signature and integrity of data by encryption.

Applying security on the IP level ensures secure communication for the applications that have security mechanisms as well as for the security ignorant applications. Internet Protocol Security (IPSec) provides encryption and authentication to all traffic at the IP level with the help of strong cryptography. Authentication and encapsulation are two basics of IPSec. Two protocols that provide authentication and encapsulation are Authentication Header (AH) and Encapsulation Security Payload (ESP). These two protocols are used in combination or alone to provide the desired set of security services for the IP layer.

The web is visible to everyone. Browser side risks and wrong configuration in web servers are some types of risks that help intruders to unauthorized remote access and interception of data. SSL is one of the most commonly used security mechanisms available on the Internet. Like other security protocols SSL is also based on cryptography. After SSLv3, Internet Engineering Task Force (IETF) renamed it TLS. SSL/TLS encrypts the data at the transport layer. Instead of HTTP port 80, SSL comes up with a special URL identity "HTTPS" which uses port 443 to establish a secure SSL session. SSL-supported browsers are used mostly for sensitive data like credit card information. TLS provides end-to-end authentication and then secure communication using cryptography.

Secure Electronic Transaction (SET) is a security protocol designed for protecting credit card transactions over the Internet. For confidentiality of information and integrity of data DES and RSA are used with SHA-1 hash codes. X.509v3 certificate is used for authentication of cardholder account and merchant account. Privacy is achieved through dual signatures.

System-level security solutions are divided into IDS, IPS, antivirus applications, firewalls, and honeypots.

The Intrusion Detection System (IDS) detects any unauthorized access or intrusion in a system or network. It is a security solution that has a passive position in a system or a network against intrusions. In a network deployment, the function of the IDS is to monitor the traffic or the network activity without impacting the traffic [19]. It means that an IDS in a network only detects or identifies any changes in the network but does not perform a resistive action against such changes.

The Intrusion Prevention System (IPS) performs the role of protection against intrusions that occur in a network or local system. It works based on the output of IDS system log files. Due to this reason, the IPS system is an extension of the IDS system. Unlikely IDS, IPS works in an active mode. IPS acts when it founds any packet dropping or unauthorized connection [20, 21].

A firewall is a barrier that performs isolation between two different networks or systems. It decides which kind of traffic can pass through a network and in which direction. Firewalls provide an additional level of defense providing the capabilities to add much tighter and more complex rules of communication between different network segments or zones [14]. Firewalls can be divided into four categories: packet filter, application gateway, circuit-level gateway, and stateful filer firewall [1, 22, 23].

A honeypot is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems. The function of a honeypot is to represent itself on the internet as a potential target for attackers, usually a server or

other high-value asset, and to gather information and notify defenders of any attempts to access the honeypot by unauthorized users.

6. CONCLUSION

Security is not about a specific firewall, product, brand, and operating system. Properly configured firewalls, strong passwords that are changed on regular basis, antivirus updates regularly, etc., all these elements are used collectively for good security practices. Each organization, depending on its business needs, budget constraints, and organizational requirements, needs to draw up a security policy and that policy will determine the mix of components that need to be installed, to meet security goals. Deficiencies in bad products can be defeated with good practice, whereas bad processes can dilute otherwise excellent products. It is better to have no security devices instead of incorrectly configured security devices. Sometimes deployment of security can affect the QoS of the network. The bottom line is that a network cannot be 100% secure. However, by analyzing the network the security level can be increased. This analysis will help to find out the vulnerabilities in the network.

"The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable." – Sun Tzu.

REFERENCES

[1] Stallings, W. (2017): *Network Security Essentials Applications and Standards,* , 6th Edition, Pearson Education, Inc.

[2] Yang, X., Euchner, M., Sebek, G., Bertine, H., Kremer, A., Youl Youm, H., Hee Oh, K., Harrop, M. (2020): *Security in Telecommunications and Information Technology*, International Telecommunication Union, 7.

[3] Osanaiye, O. A. (2015): IP spoofing detection for preventing DDoS attack in Cloud Computing, *18th International Conference on Intelligence in Next Generation Networks*, pp. 139–141. DOI: 10.1109/ICIN.2015.7073820

[4] Vacca, J. R. (2017): *Computer and Information Security Handbook*, Morgan Kaufmann.

[5] Brenner, W. Susan (2020): *Cybercrime and evolving threats from cyberspace*, 2nd Edition, Praeger.

[6] Jha, M., Anand C. S., Mahawar, Y., Kalyan, U., Verma, V. (2021): Cyber Security: Terms, Laws, Threats and Protection, *International Conference on Computing Sciences (ICCS)*, pp. 148–151.

[7] Melnik Sergey, Smirnov Nikolay, Erokhin Sergey (2017): Cyber security concept for Internet of Everything (IoE), *Systems of Signal Synchronization, Generating and Processing in Telecommunications (SINKHROINFO)*, pp. 1–4, DOI: 10.1109/SINKHROINFO.2017.7997540

[8] Bailey, Matthew (2015): *Complete Guide to Internet Privacy, Anonymity and Security*, 2nd Edition, Nerel Online,.

[9] Piper, Ben (2017): *Cisco Network Administrator*, Manning.

[10] Watts. Neal A., (2012): *Packet Analysis of Unmodified Bluetooth Communication Devices*, BiblioScholar.

[11] Harwood, Mike (2015): *Internet Security: How to Defend Against Attackers on the Web*, 2nd Edition, Jones & Bartlett Learning.

[12] Singh Chauhan Ajay (2018): *Practical Network Scanning: Capture network vulnerabilities using standard tools such as Nmap and Nessus*, Packt Publishing.

[13] Gbouri El, Sam (2018): *The 2016 Dyn DDOS Cyber Attack Analysis: The Cyber Attack that Broke the Internet for a Day*, CreateSpace Publishing Platform.

[14] Du, David (2020): *Preventing DDoS Attacks Using I Ptables* Linux server.

[15] Rahalkar, Sagar (2018): *Network Vulnerability Assessment: Identify security loopholes in your network's infrastructure*, Packt Publishing.

[16] Duraiswamy, K., Rani R., Uma (2017): *Security through Obscurity*.

[17] Gilchrist, Alasdair (2017): *A Concise Guide to SSL/TLS for DevOps*, 2nd Edition.

[18] Spivey, B., Echeverria, J. (2015); *Hadoop Security: Protecting Your Big Data Platform*, O'Reilly Media.

[19] Kim, K., Aminanto, M. E., Tanuwidjaja, H. C. (2018): *Network Intrusion Detection using Deep Learning*: *A Featurwe Learning Approach*, Springer, Singapore.

[20] Oke, J. T., Agajo, J., Nuhu, B. K., Kolo, J. G., Ajao, L. (2018): Two Layers Trust-Based Intrusion Prevention System for Wireless Sensor Networks, *Advances in Electrical and Telecommunication Engineering*, 1, pp. 23–29.

[21] Brotherston L., Berlin A. (2017):: *Defensive Security Handbook*, O'Reilly Media.

[22] Stewart, M. J. (2020): *Network Security, Firewalls, and VPNs*, 3rd Edition, Jones & Bartlett Learning.

[23] Jithin, A. (2018): *Being a Firewall Engineer: An Operational Approach: A Comprehensive guide on firewall management operations and best practices*.

Journal of Electrical Engineering and Information Technologies, Vol. **7,** No. 2, pp. 77–85 (2022)
Article 198 In print: ISSN 2545–4250
Received: October 29, 2022 On line: ISSN 2545–4269
Accepted: November 15, 2022 UDC: 004.62.057.8-049.7
DOI: https://doi.org/10.51466/JEEIT2272198077t

Original scientific paper

BIGQUERY FOR BIG DATA ANALYSIS

Žaneta Trenčeva, Aleksandar Risteski, Toni Janevski, Borislav Popovski

Faculty of Electrical Engineering and Information Technologies,
"Ss. Cyril and Methodius" University in Skopje,
Rugjer Bošković bb, P.O. Box 574, 1001 Skopje, Republic of North Macedonia
zanetatrenceva1@yahoo.com

A b s t r a c t: In todays digital era, enormous amounts of data from various sources are generated daily. This data, also known as big data, is too complex to be managed using traditional data management systems. As a result, many technologies capable of handling big and complex data have emerged in the industry. One of them is Google Cloud's BigQuery. Designed to overcome the problem of traditional databases, the BigQuery platform offers storage and analysis of big data, while providing high scalability and reliability. We will be using BigQuery to gain insights into the content ratings of an OTT (Over-The-Top) TV platform.

Key words;; analysis; content; data; query; storage

BIGQUERY ЗА АНАЛИЗА НА ГОЛЕМИ ПОДАТОЦИ

А п с т р а к т: Во денешната дигитална ера огромни количества податоци од најразлични извори се генерираат на дневно ниво. Овие податоци, познати и како „големи податоци", се премногу комплексни за да бидат менаџирани користејќи традиционални системи за управување со податоци. Како резултат, во индустријата се појавија многу технологии способни да се справат со обемни и комплексни податоци. Една од нив е BigQuery на Google Cloud. Дизајнирана да го надмине проблемот на традиционалните бази на податоци, платформата BigQuery нуди складирање и анализа на големи податоци, притоа обезбедувајќи висока скалабилност и доверливост. Ние ќе го користиме BigQuery за да добиеме увид во гледаноста на содржините на една OTT (Over-The-Top) телевизиска платформа.

Клучни зборови: анализа; содржина; податоци; барање; складирање

1. INTRODUCTION

In the past, solutions for big data management were not simple or cheap. Not only did businesses need to make a huge upfront investment in hardware and software, they also had to bring experts in data analytics into their staff too. Today, the huge amount of data in any business has forced companies to look for new, innovative solutions to this problem. One of them is Google's BigQuery, a fully managed, cloud-based serverless data warehouse. Essentially, the system works by supporting analytics strategies in a huge-scale data environment.

BigQuery is a fully managed enterprise data warehouse designed to help organizations manage and analyze their data with built-in features like machine learning, geospatial analysis, and business intelligence. BigQuery's serverless architecture lets its users use SQL queries to answer their organization's biggest questions with no infrastructure management. Its scalable, distributed analysis engine can provide querying terabytes in seconds and petabytes in minutes.

Big Query interfaces include Google Cloud console interface and the BigQuery command-line tool. Developers and data scientists can use client libraries with familiar programming including Python, Java, JavaScript, and Go, as well as BigQuery's REST API and RPC API to transform and manage data.

This paper is organized in the following manner. Section 2 provides an overview of prior related work on this topic. Section 3 describes the principles of operation of BigQuery, namely the technologies and algorithams it uses to handle Big Data. The topic of section 4 are the BigQuery concepts, that is, how the data stored in BigQuery is structured, what operations can be run on it, what data

types are supported and so on. These concepts are explained by making comparisons with traditional relational databases, such as MySQL, due to the similarities between the two types of systems. Section 5 is a demonstration of a practical usage of BigQuery, using simulated data from an OTT (Over-The-Top) TV application, resulting in insights into the ratings of its content. In section 6, the usage of the PHP Client library for the BigQuery API is presented, to demonstrate how data stored in BigQuery can be accessed from a PHP web application. Section 7 concludes this paper.

2. RELATED WORK

There are many research papers regarding BigQuery for big data manipulation. In [1], a simple approach of using BigQuery for storing and analyzing data is illustrated. In the study, data samples in CSV format are taken from a publicly available pool and imported into BigQuery. Then, this data is queried from the GCP (Google Cloud Platform) console, where the results are shown as well. Reference [2] presents a method of managing and handling non-relational data in BigQuery and calculating the execution time of queries. This paper only covers the analysis time with the dataset's size using Google SDK (Software Development Kit) rather than extracting the taken dataset's necessary values. Reference [3] validates the use of big data and cloud technologies in education related analytical applications, which are also called educational intelligence applications. It presents a prototype, which is a modified version of an open-source tool called BigQuery Visualizer. The prototype is a web application that is used to make queries to a BigQuery dataset and create plots and graphs for analytical applications. Reference [4] details the functionality of edx2bigquery – an open source Python package developed by Harvard and MIT to ingest and report on hundreds of course datasets from edX (an online course provider created by Harvard and MIT), making use of BigQuery to handle multiple terabytes of learner data. The authors find that BigQuery provides ease of use in loading the multifaceted MOOC (Massive Open Online Course) datasets and near real-time interactive querying of data, including large clickstream datasets. Moreover, flexible research and reporting dashboards are provided by visualizing and aggregating data, using services associated with BigQuery. In [5] the authors present and evaluate a novel and efficient RDF (Resource Description Framework) dictionary compression algorithm, where BigQuery is used to store and query the compressed data. The proposed algorithm is faster, generates small dictionaries that can fit in memory and results in better compression rate when compared with other large scale RDF dictionary compression algorithms. Consequently, it reduces the BigQuery storage and query costs. Reference [6] offers an overview of Explainable AI in BigQuery ML, using as an example a (fictional) realtor's linear regression model that predicted a home's latest sale price based on predictor variables such as the total tax assessment from the year of the last sale, the square footage of the house, the number of bedrooms, the number of bathrooms, and whether the condition of the home is below average. After training the linear model, the feature attribution can be studied from a global and local perspective in BigQuery.

3. PRINCIPLES OF OPERATION

BigQuery can handle a sheer amount of data while looking mostly like any other SQL database (like MySQL). How can BigQuery do what MySQL cannot? We will start by looking at the problem's two parts. First, if we need to filter billions of rows of data, we need to do billions of comparisons, which require a lot of computing power. Second, we need to do the comparisons on data that is stored somewhere, and the drives that store that data have limits on how quickly it can flow out of them to the computer that is doing those comparisons. Those two problems are the fundamental issues that need to be solved, so we will look at how BigQuery tries to address each of them [7].

a) *Scaling computing capacity*

People originally tackled the computation aspect of this problem by using the MapReduce algorithm, where data is chopped into manageable pieces and then reduced to a summary of the pieces. This speeds up the entire process by parallelizing the work to lots of different computers, each working on some subset of the problem. For example, if we had a few billion rows and wanted to count them, the traditional way to do this would be to run a script on a computer that iterates through all the rows and keeps a counter of the total number of rows, which would take a long time. Using MapReduce, we could speed this up by using 1,000 computers, with each one responsible for counting one one-thousandth of the rows, and then summing up the 1,000 separate counts to get the full count (Figure 1).

In short, this is what BigQuery does under the hood. Google Cloud Platform has thousands of CPUs in a pool dedicated to handling requests from BigQuery. When we execute a query, it momentarily gives us access to that computing capacity, with each unit of computing power handling a small

piece of the data. Once all the little pieces of work are done, BigQuery joins them all back together and gives us a query result.

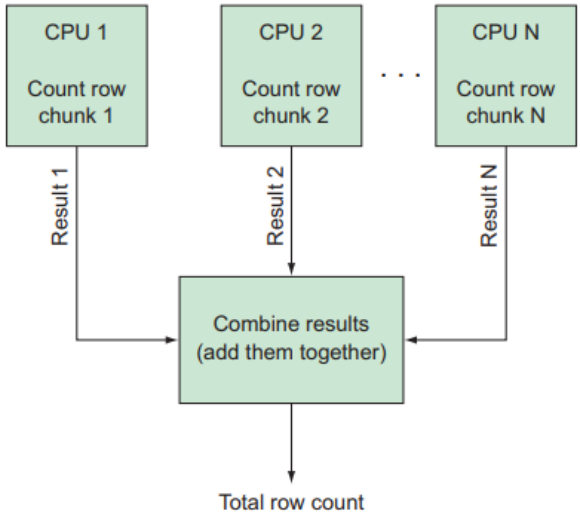


Fig. 1. Counting a few billion rows by breaking them into chunks

b) *Scaling storage throughput*

When we solved the computational capacity problem by splitting the problem up into many chunks and using lots of CPUs to crunch on each piece in parallel, we never thought about how we would make sure all of the CPUs had access to the chunks of data. If these thousands of CPUs all requested the data from a single hard drive, the drive would get overwhelmed in no time. The problem is compounded by the fact that the total amount of data you need to query is potentially enormous.

To make this more concrete, most drives, regardless of capacity, typically can sustain hundreds of megabytes per second of throughput. At that rate, pulling all the data off of one 10-terabyte (TB) drive (assuming a 500 MB/s sustained transfer rate) would take about five hours. If 1,000 CPUs all asked for their chunk of data (1,000 chunks of 10 GB each), it would take about five hours to deliver them, with a best case of about 20 seconds per 10 GB chunk. The single disk acts as a bottleneck because it has a limited data transfer rate.

To fix this, the database could be splitted across lots of different physical drives (called "sharding") (Figure 2) so that when all of the CPUs started asking for their chunks of data, lots of different drives would handle transferring them. No drive alone would be able to ship all the bytes to the CPUs, but the pool of many drives could ship all that data quickly. For example, if we were to take those same 10 TB and split them across 10,000 separate drives, 1 GB would be stored on each drive. Looking at the fleet of all the drives, the total throughput available would be around 5 TB/s. Also, each drive could ship the 1 GB it was responsible for in around two seconds. Regarding the example with 1,000 separate CPUs each reading their 10 GB chunk (one one-thousandth of the 10 TB), they would get the 10 GB in two seconds-each one would read ten 1 GB chunks, with each chunk coming from one of 10 different drives.

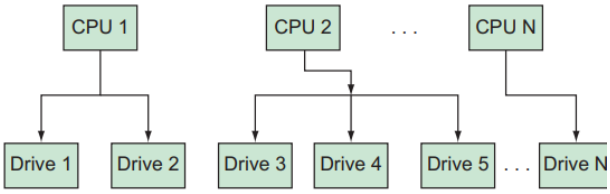


Fig. 2. Sharding data across multiple disks

Under the hood, Google is doing this, using a custom-built storage system called Colossus, which handles splitting and replicating all of the data.

4. CONCEPTS

As already mentioned, BigQuery is very SQL-like, so close comparisons can be drawn with things the reader is most probably familiar with in systems like MySQL [7].

a) *Datasets and tables*

Like a relational database has databases that contain tables, BigQuery has datasets that contain tables (Figure 3). The datasets mainly act as containers, and the tables, again like a relational database, are collections of rows. Unlike a relational database, the user does not necessarily control the details of the underlying storage systems, so although datasets act as collections of tables, one has less control over the technical aspects of those tables than they would with a system like MySQL or PostgreSQL.

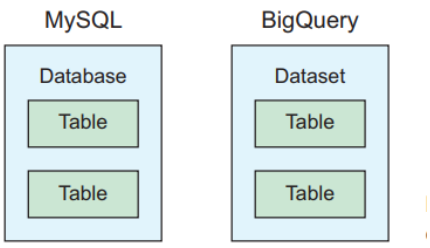


Fig. 3. A BigQuery dataset and tables compared to a MySQL database and tables

Each table contained in the dataset is defined by a set schema, so BigQuery can be thought of in a traditional grid, where each row has cells that fit the types and limits of the columns defined in the schema. It gets a little more complicated than that when a particular column allows nested or repeated values, but we will explore that in more detail later in this paper.

Unlike in a traditional relational database, BigQuery rows typically do not have a unique identifier column, primarily because BigQuery is not meant for transactional queries where a unique ID is required to address a single row. Because BigQuery is intended to be used as an analytical storage and querying system, constraints like uniqueness in even a single column are not available. Otherwise, BigQuery will accept most common SQL-style requests, like SELECT statements, UPDATE, INSERT, and DELETE statements with potentially complex WHERE clauses, as well as JOIN operations.

b) *Schemas*

As with other SQL databases, BigQuery tables have a structured schema, which in turn has the standard data types, such as INTEGER, TIMESTAMP, and STRING (sometimes known as VARCHAR). Additionally, fields can be required or nullable (like NULL or NOT NULL). Unlike with a relational database, we define and set schemas as part of an API call rather than running them as a query.

For example, we might have a table of people with fields for each person's name, age, and birth date, but instead of running a query that looks like CREATE TABLE, we would make an API call to the BigQuery service, passing along the schema as part of that message. We can represent the schema itself as a list of JSON objects, each with information about a single field. In the following example listing, the NULLABLE and REQUIRED (SQL's NOT NULL) are listed as the mode of the field.

```
{"name": "name",      "type": "STRING",    "mode": "REQUIRED"},
{"name": "age",       "type": "INTEGER",   "mode": "NULLABLE"},
{"name": "birthdate", "type": "TIMESTAMP", "mode": "NULLABLE"}
```

There is an additional mode called REPEATED, which is currently not common in most relational databases. Repeated fields do as their name implies, taking the type provided and turning it into an array equivalent. A repeated INTEGER field acts like an array of integers. BigQuery comes with special ways of decomposing these repeated fields, such as allowing us to count the number of items in a repeated field or filtering as long as a single entry of the field matches a given value.

Next, a field type called RECORD acts like a JSON object, allowing us to nest rows within rows. For example, the people table could have a RECORD type field called favorite_book, which in turn would have fields for the title and author (which would both be STRING types). Using RECORD types like this is not a common pattern in standard SQL, where it would be normalized into a separate table (a table of books, and the favorite_book field would be a foreign key). In BigQuery, this type of inlining or denormalizing is supported and can be useful, particularly if the data (in this case, the book title and author) is never needed in a different context – it is only ever looked at alongside the people who have the book as a favorite.

5. THE TV PROJECT ON GCP CONSOLE

For our practical demonstration of BigQuery, we will be using simulated data from an OTT TV platform, an interactive TV service that allows users to watch live TV, VOD (Video On Demand), record programs and more. The TV application, which is an Android application, is integrated with Firebase, and it uses the Google Analytics for Firebase SDK. Google Analytics is an application measurement solution, that provides insight on application usage and user engagement. The SDK automatically captures a number of events and user properties, but also allows users to define their own custom events to measure the things that uniquely matter to their business. Automatically collected events are triggered by basic interactions with the application, and no additional code should be written to collect them. Some automatically collected events include: "first_open" (the first time a user launches an application after installing or re-installing it), "user_engagement" (when the application is in the foreground for at least one second), "dynamic_link_app_open" (when a user re-opens the application via a dynamic link), etc.

To the contrary, custom events are defined by the developer of the application, by explicitly writing code in the desired places in the program, that will include the custom event name and (optionally) custom event parameters. In our practical example, we will be working with custom events.

When users watch content on our OTT TV platform, they generate a large amount of different events. In the application, there is code that "catches" these user interaction events that can be, for example, changing a channel, scheduling a recording of a program, interacting with a menu, pausing or rewinding a live channel, etc. All this data,

that in fact represents user behaviour, is available in Google Analytics, and since the Firebase project is linked to BigQuery, it is also stored in a dedicated project in BigQuery.

We can open our BigQuery project in the GCP console. The console provides a graphical interface used to create and manage BigQuery resources and run SQL queries.

Figure 4 is a screenshot of the "SQL workspace" section of the BigQuery page of our project in the console. It consists of an Explorer pane and a Details pane.

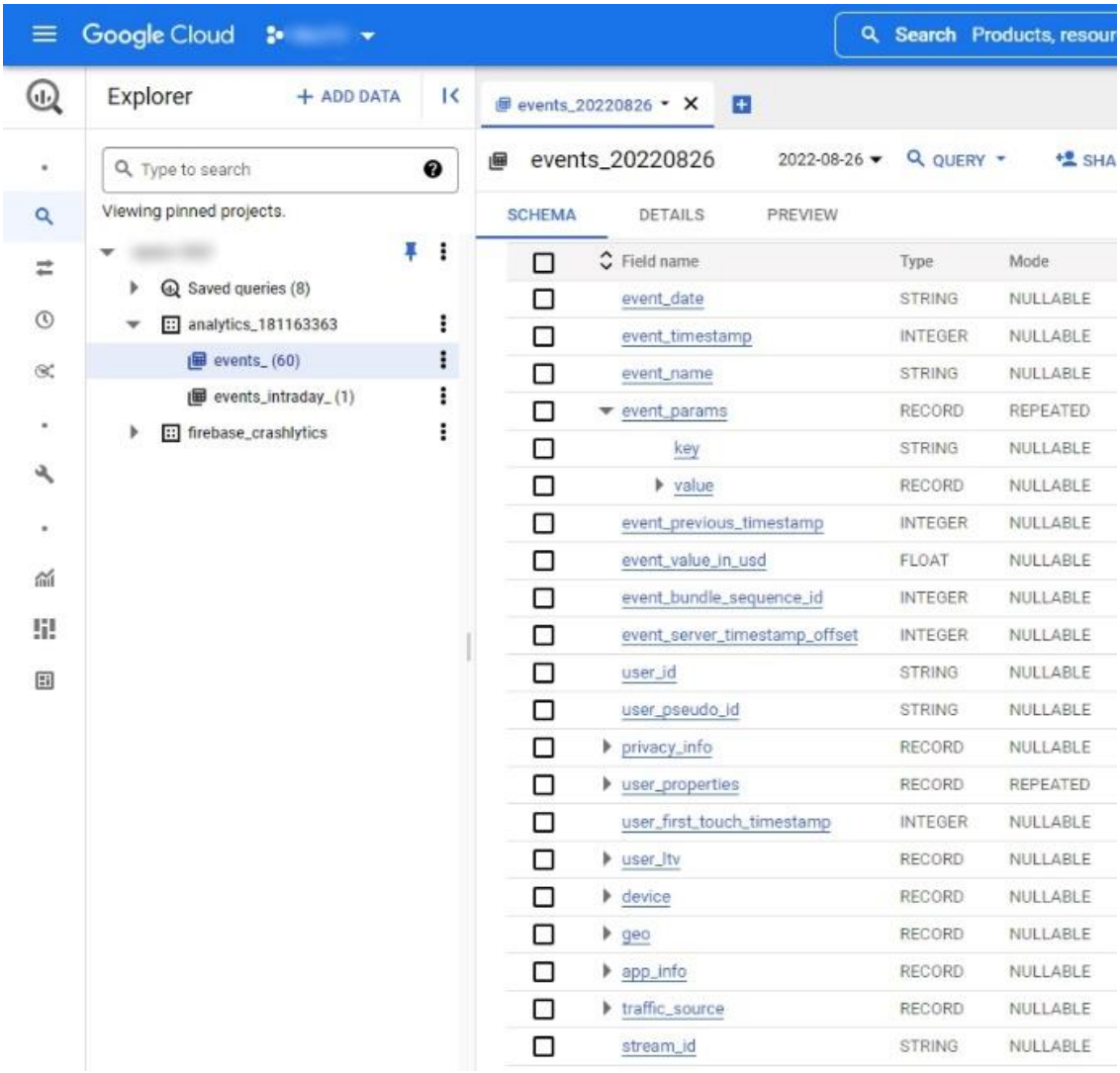


Fig. 4. The BigQuery dashboard of the TV project

The Explorer pane lists current Cloud projects and any pinned projects. Datasets can be accessed by expanding the project, and tables, views and functions can be accessed by expanding the dataset.

The Details pane shows information about the BigQuery resources. When we select a dataset, table, view, or other resource in the Explorer pane, a new tab is displayed. On these tabs, we can view information about the resource, create tables and views, modify table schemas, execute SQL queries, export data, and perform other actions.

For each Firebase project that is linked to BigQuery, a single dataset named "analytics_<property_id>" is added to the BigQuery project. Property ID refers to the Analytics Property ID, which can be found in App Analytics Settings in the Firebase project.

Regarding dataset structure, within each dataset, a table named "events_YYYYMMDD" is created each day whether the Daily export or Streaming export option is enabled (during the Firebase integration process). Moreover, if the Streaming export option is enabled, an additional table, "events_intraday_YYYYMMDD", is created. This table is populated continuously as events are recorded throughout the day. It is deleted at the end of each day once "events_YYYYMMDD" is complete.

That being said, we can now explore our project. The project contains two datasets, "analytics_181163363" and "firebase_crashlytics", as well as several saved queries.

We are interested in the "analytics_181163363" dataset. It contains 60 tables named "events_YYYYMMDD", which store events that happened on the specific date in the past 60 days. There is also the "events_intraday_YYYYMMDD" table, which stores events happening on the current day, as we previously explained. Figure 4 also shows a part of these tables' schema, that is, the fields (table columns), their types and their modes. For example, the field "event_name" is of type STRING and it is NULLABLE. The field "event_params", on the other hand, is of type RECORD, and it is in REPEATED mode. That means that it acts as an array of struct types, that is, there can be many entries within this field, and each of them will have both "key" and "value".

By examining the table's fields, we can conclude that these tables store various information, such as information about the triggering event, the user, the user device, the application, geo location etc. The schema of these tables, that is, the fields, is defined by Google Analytics, and not by the user. The user can, however, specify event parameters for their custom events.

Next to the Schema tab (that we have been examining so far) in the Explorer pane, is the Details tab, which gives some basic table information, such as its size, number of rows, expiration date etc. It is shown on Figure 5. The last tab is the Preview tab, where actual table entries are shown, sorted in descending order. Two entries with only the first several fields can be seen on Figure 6.

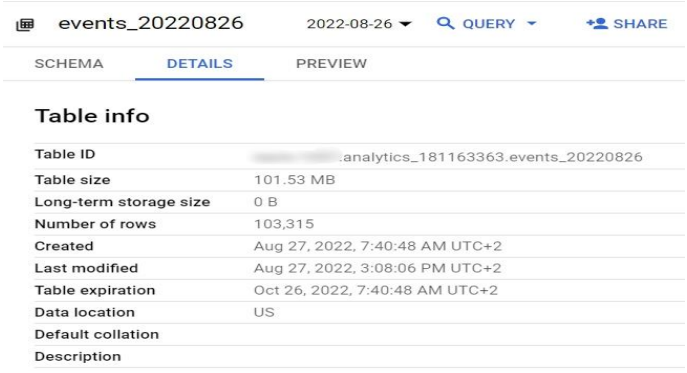


Fig. 5. Details tab of the Explorer pane

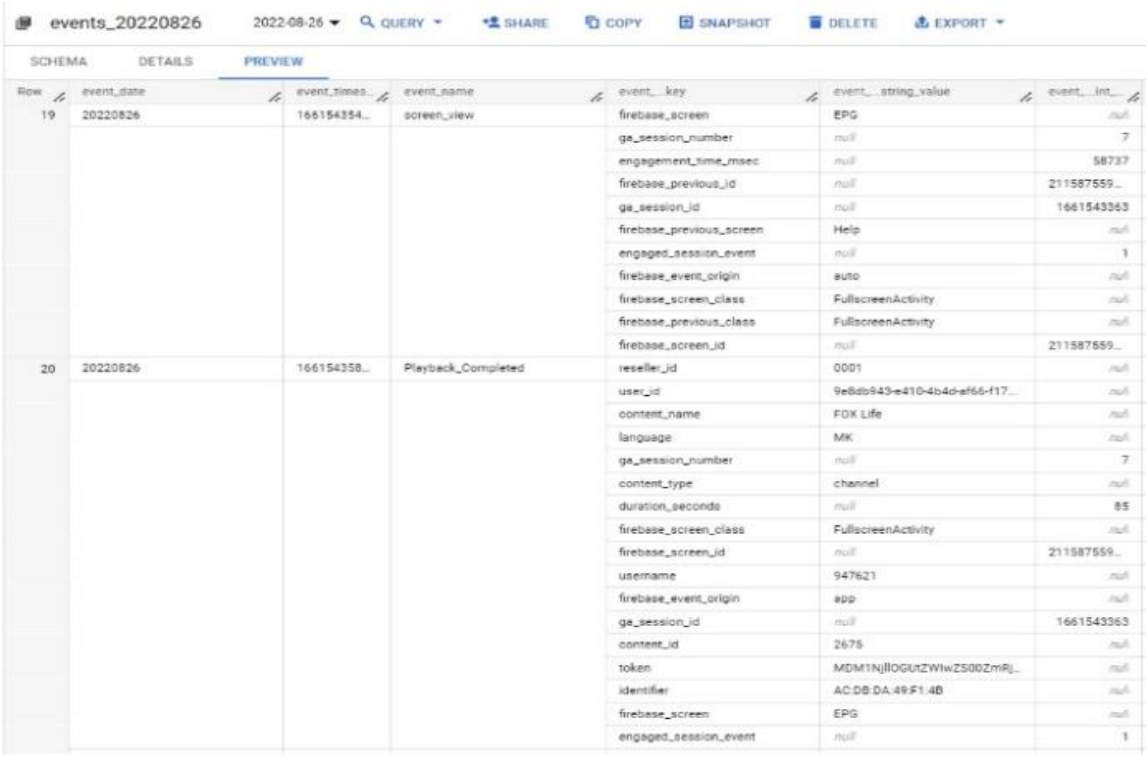


Fig. 6. Preview tab of the Explorer pane

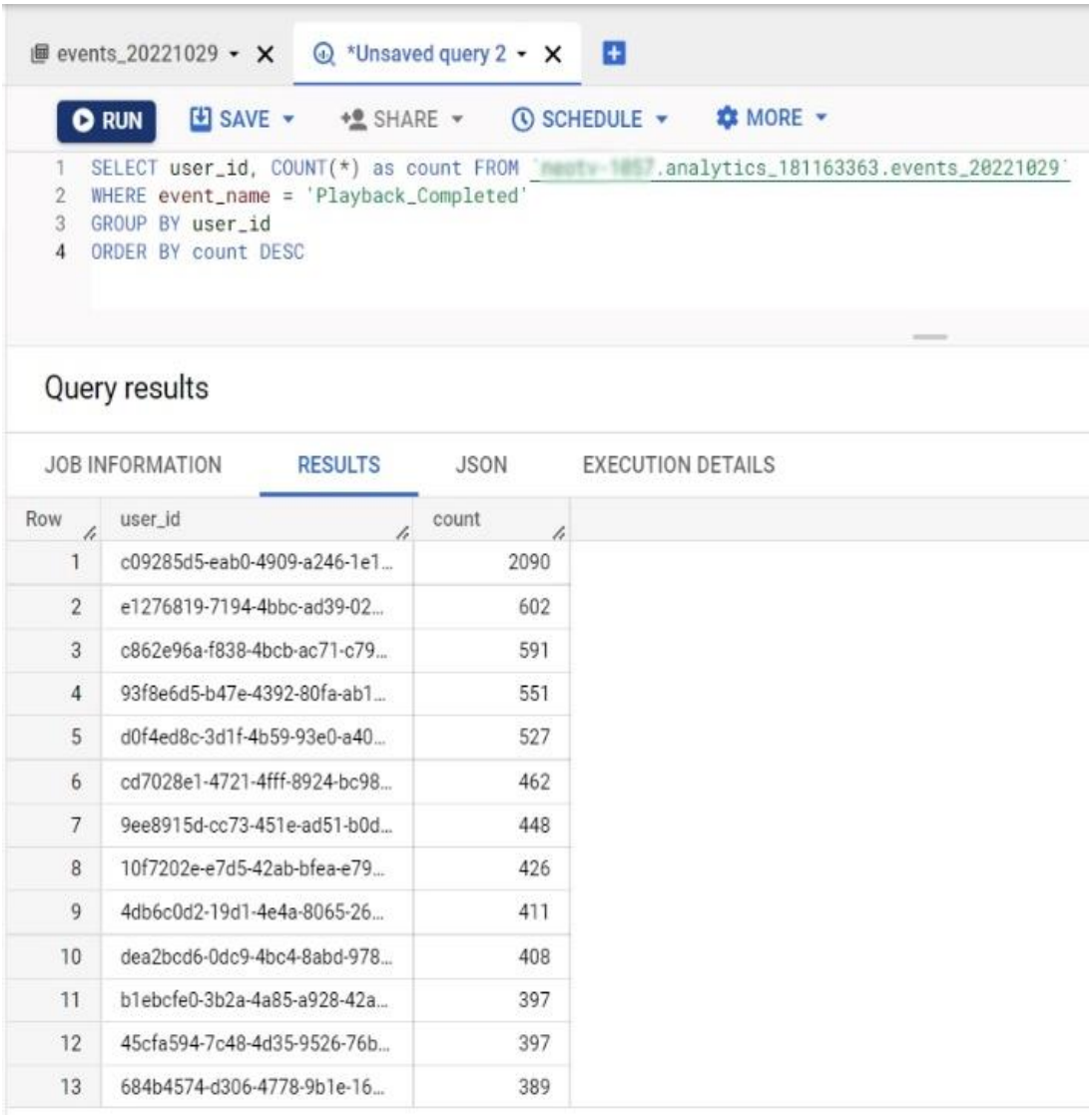
We will now demonstrate query execution in the console with two examples. In both of them we are working with custom events whose “event_name” parameter is “Playback_Completed”, as those are the events that hold data about user sessions (and therefore, content ratings).

The first query and part of its results are shown on Figure 7. The query uses the events table from 29.10.2022, and filters records whose “event_name” field is “Playback_Completed”. It then groups these records by user ID, counts them, and displays the results in descending order of the number of records.

Figure 8 shows another example of a SQL query in the console and part of its results upon execution.

In the SQL query, it can be noted that an UNNEST operator is being used. The UNNEST operator is used to convert an array into set of rows, also known as “flattening”. It takes an array and returns a table with a single row for each element in it. Basically, we are unnesting the “event_params” field (which is an array, as its mode is REPEATED) by key (“content_name”, “duration_seconds”, “content_type” and “username”).

What the query does is, it fetches results in the form of content ratings cumulatively, namely how much time a certain content was watched, and how many sessions of it occurred. It does this the following way: it uses the “Playback_Completed” events (that is, user sessions), filtered by a starting date and an ending date, the type of content watched (in this case, live channel, but can also be timeshift, VOD and radio) and grouped by the content name. Then it sums the “duration_seconds” parameter of each session to calculate the overall ratings in seconds (hours) of the given content, and counts the “content_name” parameter (or any other from the “event_params” field) to determine the number of times the given content was watched. Finally, the data is ordered in descending order by the overall time a content was watched.



Row	user_id	count
1	c09285d5-eab0-4909-a246-1e1...	2090
2	e1276819-7194-4bbc-ad39-02...	602
3	c862e96a-f838-4bcb-ac71-c79...	591
4	93f8e6d5-b47e-4392-80fa-ab1...	551
5	d0f4ed8c-3d1f-4b59-93e0-a40...	527
6	cd7028e1-4721-4fff-8924-bc98...	462
7	9ee8915d-cc73-451e-ad51-b0d...	448
8	10f7202e-e7d5-42ab-bfea-e79...	426
9	4db6c0d2-19d1-4e4a-8065-26...	411
10	dea2bcd6-0dc9-4bc4-8abd-978...	408
11	b1ebcfe0-3b2a-4a85-a928-42a...	397
12	45cfa594-7c48-4d35-9526-76b...	397
13	684b4574-d306-4778-9b1e-16...	389

Fig. 7. Query execution and results: Number of sessions by user ID

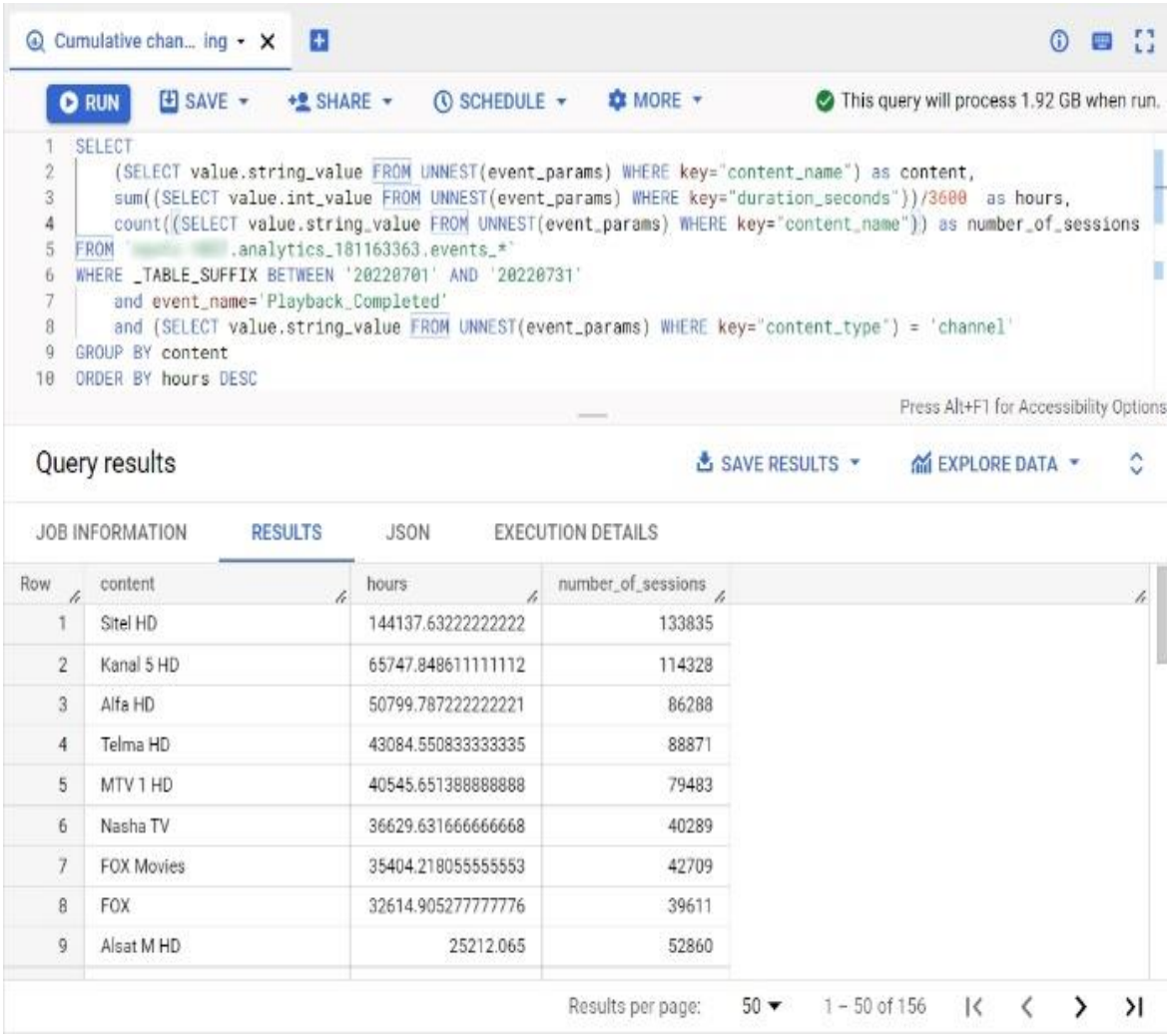


Fig. 8. Query execution and results: Watch time and number of sessions of live channels

As we can see, "Sitel" is the most watched live TV channel, with approximately 144 137 hours of watch time and 133 835 user sessions. We can visualize these results using Google Data Studio, an online tool for converting data into customizable informative reports and dashboards. We can do that by clicking the export data button and then choosing Data Studio. Figure 9 shows (a part of) the query results presented in a bar chart.

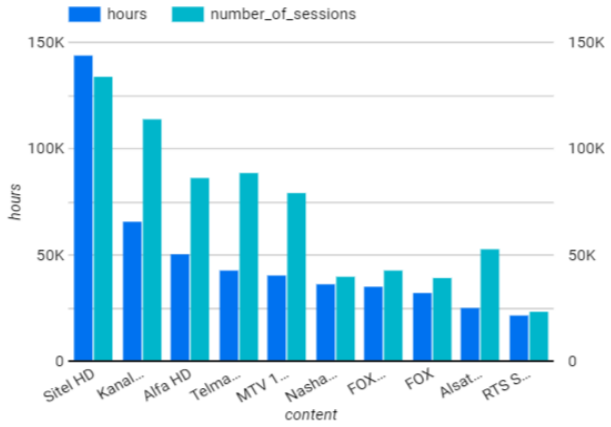


Fig. 9. Bar chart of query results in Data Studio

6. THE PHP CLIENT LIBRARY FOR THE BIGQUERY API

Google Cloud APIs are programmatic interfaces to Google Cloud Platform services, that allow users to easily add different functionalities to their applications.

Client libraries make it easier to access Google Cloud APIs from a supported language. While Google Cloud APIs can be used directly by making raw requests to the server, client libraries provide simplifications that significantly reduce the amount of code that needs to be written.

We will now take a look at how to use the PHP Client library for the BigQuery API, that is, how to access data stored in a BigQuery project from a PHP web application.

Assuming we have a PHP web application, we first need to install the client library in it. In PHP, this is done by running "composer require google/cloud-bigquery". In order to do that, we must first set up authentication. One way to set up authentication is to create a service account in the TV

project in the cloud console and then generate a service account key and download it locally. Finally, we need to make a connection to the TV project, using the generated key. The code for this purpose is the following, where the JSON file is the downloaded key:

```
<?php
require 'vendor/autoload.php';
use Google\Cloud\BigQuery\BigQueryClient;
$projectId = '<project-name>';
$path = '<project-name>-d0425aeab4c1.json';
$bigQuery = new BigQueryClient([
'projectId' => $projectId,
'keyFilePath' => $path,
]);
?>
```

The "bigQuery" variable holds the connection to the project in BigQuery and will be used to execute the SQL queries.

If we have a SQL query like the one we saw earlier in this paper, and assign it to a STRING variable called "query", we can then execute the query programmatically, using the following code:

```
$queryJobConfig = $bigQuery->query($query);
$queryResults = $bigQuery -> runQuery($query JobConfig);
```

If the query has run successfully, we have the results in the "queryResults" variable. Finally, we are extracting the "content", "hours" and "no_sessions" fields of the resulting rows and simply echoing them to the web page. The code for this purpose is the following:

```
if ($queryResults->isComplete()) {
    $rows = $queryResults->rows();
    $results = array();
    foreach ($rows as $row) {
     echo $row['content'] . ' ' . $row['hours'] . ' ' . $row['no_sessions']);
    } else {
    throw new Exception('The query failed to complete');
}
```

7. CONCLUSION

Google BigQuery is a service designed to provide its customers with insight into their businesses quickly and cost-effectively. With a company's data system located on the cloud, comes the freedom and flexibility to modernize its entire business structure. Some of the most significant advantages offered by BigQuery are:

– Accelerated time to value: Users can gain insight into their businesses as soon as they start using the service (no prior planning and implementation costs).

– Simplicity and scalability: All analytical requirements can be performed through a simple and effective interface, without additional management infrastructure. The system can scale depending on demand for performance, size and pricing.

– Speed: With BigQuery, data is processed at a tremendous speed thanks to the technologies it uses.

– Security: All projects are encrypted and protected with IAM (Identity and Access aManagement) support.

– Reliability: Google Cloud and BigQuery enable access to always-on servers, and geographic replication across a huge selection of Google data centers around the world.

Throughout this paper, we saw the benefits of BigQuery in action. The example solution we presented for storage and analysis of OTT TV platform data can prove very useful for business analysts of the platform, as it provides information on which specific content has the most watch time and which has the least.

REFERENCES

[1] Ali, H., Hosain, S., Hossain, A. (2021): Big Data analysis using BigQuery on cloud computing platform, *Australian Journal of Engineering and Innovative Technology*, **3** (1), pp. 1–9.

[2] Kotecha, B., Joshiyara, H. (2018): Handling non-relational databases on Big Query with scheduling approach and performance analysis", *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, pp. 118–127.

[3] Khan, S., Alam, M. (2018): Analyzing Big 'Education' Data using BigQuery and R, *8th DBT-BIF National Workshop on Translational Bioinformatics: Bench-to-Bedside*, Department of Computer Science, April 9–10;

[4] Lopez, G., Seaton, D., Ang, A., Tingley, D., Chuang, I. (2017): Google BigQuery for education: Framework for parsing and analyzing edX MOOC data, *Proceedings of the Fourth (2017) ACM Conference on Learning @ Scale*, pp. 181–184.

[5] Dawelbeit, O., Mccrindle, R. (2016): Efficient dictionary compression for processing RDF Big Data using Google BigQuery, *2016 IEEE Global Communications Conference.* 10.1109/GLOCOM.2016.7841775.

[6] Lichtendahl, K. C., Boatright, B. (2022): Google Cloud Platform: BigQuery Explainable AI, Darden Case No. UVA-QA-0943.

[7] Geewax, J. J. (2018): *Google Cloud Platform in Action*, Manning Publications, USA.

Journal of Electrical Engineering and Information Technologies, Vol. **7,** No. 2, pp. 87–96 (2022)
Article 199
Received: November 21, 2022
Accepted:December 5, 2022
In print: ISSN 2545–4250
On line: ISSN 2545–4269
UDC: 681.5.037.26:519.71
DOI: https://doi.org/10.51466/JEEIT2271199087d

Original scientific paper

Dedicated to late Professor Milčo Kocare, the great teacher of Electronics, Communications and Automation, while honoring our colleagues Goce Arsov and Ljupčo Panovski and the hospitality of FEIT Institutes of Electronics and of Automation & Systems Engineering

STATE FEEDBACK H_∞ CONTROL FOR A CLASS OF SWITCHED FUZZY SYSTEMS

Georgi Marko Dimirovski[1], **Yuanwei Jing**[2]

[1]*Faculty of Electrical Engineering and Information Technologies,*
"Ss. Cyril and Methodius" University in Skopje,
Rugjer Bošković bb, P.O. Box 574, 1001 Skopje, N. Macedonia
[2]*Northeastern University in Shenyang, College of Information Science and Engineering,*
Shenyang 110004 Liaoning, P.R. China
dimir@feit.ukim.edu.mk // jingyuanwei@ise.neu.edu.cn

A b s t r a c t: An innovated model of the switched fuzzy systems whose subsystems are fuzzy systems is presented. State feedback H_∞ control for this class of fuzzy systems is studied using theory of switching systems and control by employing single Lyapunov function technique. A switching strategy of the switched fuzzy system with continuous-time control input and a relevant switching law is developed. The main condition for asymptotic stability of the equilibrium state is given in form of convex combinations of linear matrix inequalities, which are solvable by LMI Toolbox and Matlab-Simulink platform. Application to a room regulated air-conditioning plant and the respective simulation results are presented to demonstrate the effectiveness and feasible operating performance of the hybrid control design.

Key words;; switching control; fuzzy logic control; switched fuzzy systems;, state feedback H_∞ control

СОСТОЈБЕНО H_∞ УПРАВУВАЊЕ ПО ПОВРАТНА ВРСКА ЗА КЛАСА НА ПРЕВКЛУЧУВАЧКИ ФАЗИ-СИСТЕМИ

А п с т р а к т: Трудот презентира иновиран модел на превклучувачки фази-системи чии потсистеми се исто така фази-системи. Проучувано е состојбено H_∞ управување по повратна врска за оваа класа на системи со користење на теоријата на превклучувачки системи и на техниката на единична функција на Љапунов. Развиени се превклучувачка стратегија за превклучувачкиот фази-систем со континуиран управувачки влез и соодветен закон за превклучување. Главниот услов за асимптотска стабилност на рамнотежната состојба е даден во облик на конвексни комбинации на линеарни матрични неравенства кои се решаваат со LMI Toolbox во платформата Matlab-Simulink. Презентирана е апликација на ваквиот пристап при управување на процес за кондиционирање на воздух во затворена просторија, како и соодветни симулациски резултати. Со тоа се демонстрираат остварливоста и ефикасноста на изложениот хибриден дизајн на управување.

Клучни зборови: превклучувачко управување; фази логичко управување; превклучувачки фази-системи; состојбено H_∞ управување по повратна врска

1. INTRODUCTION

In recent years, considerable attention has been paid to analysis and synthesis of switched systems [1–4]. Switched systems represent one important class of hybrid systems [5, 22, 23]. A switched system consists of a number of sub-systems, either continuous- or discrete-time dynamic systems, along with a relevant switching law that orchestrates the switching between its sub-systems.

Important applications such as in computer disc drives [5], some robot control [6], cart-pendulum systems [7], and recent aero-space developments emphasized switched systems have extensive engineering background in practice in particular [18, 19]. Their theoretical significance and practical value paved a flourishing trend to study switched systems.

On the other hand, fuzzy logical control [8, 24, 25] has emerged as one of the most active and fruitful areas. In the recent past, certain rather useful techniques for stability analysis and synthesis have emerged due to the methodology of Linear Matrix Inequalities (LMI), its scientific background and its computing technology. The LMI-based designs for Takagi-Sugeno (T-S) fuzzy systems have sparked a trend toward the fuzzy control theory and design techniques [8, 20–22]. The LMI techniques are employed to solve an H_∞ control problem of a nonlinear control system via robust H_∞ fuzzy control [9]. A thorough study of stability analysis and synthesis of nonlinear time-delay systems via linear T-S fuzzy models by state feedback, includeng stabilization of uncertain fuzzy systems, has been explored in [10, 11] by using the LMI techniques. In particular, the H_∞ control problem for uncertain discrete-time fuzzy systems by state feedback has been considered in [11]. In [12], the mixed H_2/H_∞ fuzzy feedback control problems using LMIs have been considered [17, 19, 25, 26], which are further developed and extended in recent studies [27, 28, 30].

A switched system is called a switched fuzzy system if all subsystems are fuzzy systems. This class of systems can often more precisely describe continuous dynamics and discrete dynamics as well as their interactions in actual systems. Compared with the results on stability of switched systems and those of fuzzy control systems, the results on switched fuzzy systems are very few. In [13], the combination of hybrid systems and fuzzy multiple model systems is described, and a fuzzy switched hybrid controller is put forward. In [14, 15], a switching fuzzy model is studied and stability conditions are given as well as [16–18] give some extension based on [14, 15]. Such a switching fuzzy system model has two levels of structure, which the first level is region rule level and the second level is a local fuzzy rule level. This model is switching in local fuzzy rule level of the second level according to the premise variable in region rule level of the first level, which promise wide applications [29, 32, 33].

An innovated model for a class of switched fuzzy systems and its fuzzy-logic based control is proposed in this paper, which differs from existing ones. It represents essentially a switched system whose sub-systems all are fuzzy systems. The respective synthesis design methods do inherit some features of hybrid systems, but involves information flow of fuzzy systems. The state feedback H_∞ robust control is investigated exploiting the idea that control infrastructure too should be derived employing a similar fuzzy-rule model to that of the plant system. In contrast to many existing results, in here studied switched fuzzy system control is rather relying on the intuitive *T-S* fuzzy-rule models.

This approach provides a kind of different premise variable switching directly, while works in aforementioned [14–18] considered a model with two-level structure. Synthesis design of both continuous-time controllers for subsystems and switching law has been developed. Furthermore, based on single Lyapunov function technique, a sufficient condition for the switched fuzzy systems to be asymptotically stable with H_∞-norm bound is derived. Finally, by using Matlable's Fuzzy Toolbox, LMI Toolbox and Simulink, the obtained simulation results for the application to for room air-conditioning plant, on its regulating system, demonstrate the effectiveness and feasible performance of this novel control design synthesis. References follow thereafter.

2. SYSTEM MODEL AND PRELIMINARIES

Consider the continuous-time uncertain switched fuzzy model of Takagi-Sugeno class. In this class of *T-S* switched fuzzy systems every subsystem systems is an uncertain fuzzy system as follows:

$$\begin{aligned} R^l_{\sigma(t)}&: \text{if } \xi_1 \text{ is } M^l_{\sigma(t)1}\cdots \text{and } \xi_p \text{ is } M^l_{\sigma(t)p}, \text{ then} \\ &\dot{x}(t) = A_{\sigma(t)l}x(t) + B_{1\sigma(t)l}w_{\sigma(t)}(t) + B_{2\sigma(t)l}u_{\sigma(t)}(t), \\ &z(t) = C_{\sigma(t)l}x(t) + D_{\sigma(t)l}u(t), \quad l = 1,2,\cdots N_{\sigma(t)}. \end{aligned} \tag{1}$$

Quantities in (1) denote: $\xi_1, \xi_2, \cdots, \xi_p$ are the fuzzy-set premise variables;

$$\sigma(t) : R_+ \to M = \{1,2,\cdots,m\}$$

is a piecewise constant function, called a switching sequence signal; $M^l_{\sigma 1}, \cdots, M^l_{\sigma p}$ denote fuzzy sets

in the σ-th switched subsystem; $R^l_{\sigma(t)}$ denotes the l-th fuzzy inference rule in the σ-th switched subsystem; $N_{\sigma(t)}$ is the number of inference rules in the σ-th switched subsystem such that fuzzy rules are selected in every switched subsystem; $u_{\sigma(t)}(t)$ is the control input of the σ-th switched subsystem; $x(t)$ is the system state variable vector, $z(t)$ is the output to be controlled, while $w_{\sigma(t)}(t)$ is disturbance input of the σ-th switched subsystem; matrices $A_{\sigma(t)l}$, $B_{1\sigma(t)l}$, $B_{2\sigma(t)l}$ and $C_{\sigma(t)l}, D_{\sigma(t)l}$ are known constant matrices of appropriate dimensions of the σ-th switched subsystem.

It should be noted further that the i-th switched subsystem appears in the form:

$$\begin{aligned} R^l_i:\ &\text{if } \xi_1 \text{ is } M^l_{i1}\cdots\text{and } \xi_p \text{ is } M^l_{ip}, \text{ then}\\ &\dot{x}(t) = A_{il}x(t) + B_{1il}w_i(t) + B_{2il}u_i(t),\\ &z(t) = C_{il}x(t) + D_{il}u(t),\\ &l = 1,2,\cdots N_i, \qquad i = 1,2,\cdots,m. \end{aligned} \tag{2}$$

Then global or overall model of the i-th switched subsystem via *Zadeh's fuzzy-logic inference* [24–25] is described by:

$$\begin{aligned} \dot{x}(t) &= \sum_{l=1}^{N_i}\eta_{il}(\xi(t))\left[A_{il}x(t) + B_{1il}w_i(t) + B_{2il}u_i(t)\right],\\ z(t) &= \sum_{l=1}^{N_i}\eta_{il}(\xi(t))\left[C_{il}x(t) + D_{il}u_i(t)\right],\\ i &= 1,2,\cdots,m, \end{aligned} \tag{3}$$

where:

$$0 \le \eta_{il}(\xi(t)) \le 1, \quad \sum_{l=1}^{N_i}\eta_{il}(\xi(t)) = 1 \quad . \tag{4a}$$

$$w_{il}(\xi(t)) = \prod_{\rho=1}^{p} M^l_{i\rho}(\xi_\rho(t)), \tag{4b}$$

$$\eta_{il}(\xi(t)) = [w_{il}(\xi(t))] \Big/ [\sum_{l=1}^{N_i} w_{il}(\xi(t))]. \tag{4c}$$

Notice, in here, quantity $M^l_{i\rho}(\xi_\rho(t))$ denotes the fuzzy-set membership function and $\xi_\rho(t)$ belon gs to the fuzzy set $M^l_{i\rho}$.

Now, H_∞ control problem for the switched fuzzy system (1) can be stated as follows:

Let a constant $\gamma > 0$ be given. Find a continuous-time state-feedback controller $u_i = u_i(x)$ for each sub-system, and a relevant switching law $i = \sigma(t)$ such that:

(1) The closed-loop control system is asymptotically stable whenever $w_i = 0$.

(2) The output z satisfies $\|z\|_2 \le \gamma\|w_i\|_2$ beginning with zero initial condition, which is typical driving mode to operating steady-state equilibrium.

Fuzzy systems partition the state space into many fuzzy sub-areas, and local model is designed in every fuzzy sub area. Global model of fuzzy system is composed of a series of local model which is linked by fuzzy membership function. If all the sub-systems of the considered switched system are all *T-S* fuzzy systems (or any other class of fuzzy system models for that matter), then such systems represent the class of switched *T-S* fuzzy systems.

In fact, a sketch map of the switched fuzzy systems is depicted in Figure 1 where Ω_i denotes the system state area of the i-th switched subsystem. Ω_{il} denotes the l-th fuzzy sub-area in Ω_i. It should be noted again, the switched fuzzy system partitions the Ω_i sub-area into l fuzzy sub-areas $\Omega_{i1},\cdots,\Omega_{il},\cdots,\Omega_{i\ell}$. There is local linear model in every fuzzy sub-area, namely local linear model in Ω_{il} is its state-space model,

$$\dot{x}(t) = A_{il}x(t) + B_{il}u_i(t).$$

The model of every switched sub-area $\Omega_1,\cdots,\Omega_i,\cdots,\Omega_m$ is composed of local linear models which are linked by the fuzzy set membership functions.

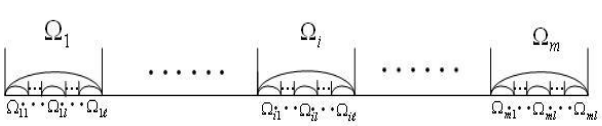


Fig. 1. A descriptive map of switched fuzzy systems in their state space

The design of the switching law for fuzzy sub-area model is carried out so as to ensure stability of the overall switched fuzzy system. When local

model in fuzzy sub-area satisfies the switching law, then the switch goes to the Ω_i -th sub-system to ensure stability of the switched fuzzy system.

3. MAIN NOVEL RESULTS

This section derives a condition for the H_∞ control problem to be solvable and presents design synthesis employing continuous-time controllers for subsystems and a switching law. Here, the methodology due to Tanaka and coauthors [14–16] for PDC fuzzy controller design is being used for every fuzzy sub-system [8].

Namely, as the plant system (2) also the fuzzy controller together both are assumed to have the same fuzzy inference premise variables. Therefore, in terms of Takagi-Sugeno fuzzy-rule models, it follows:

$$R_{ic}^{l}: \text{ if } \xi_1 \text{ is } M_{i1}^{l}\cdots \text{ and } \xi_p \text{ is } M_{ip}^{l}, \text{ then } u_i(t)=K_{il}x(t),\ l=1,2,\cdots N_i,\ i=1,2,\cdots,m. \tag{5a}$$

Thus again following Zadeh's fuzzy logic inference [14–25], globally the overall control is inferred as follows:

$$u_i(t)=\sum_{l=1}^{N_i}\eta_{il}K_{il}x(t)\ ,\ i=1,2,\cdots,m. \tag{5b}$$

Then globally the overall model of the i -th fuzzy sub-system is described by:

$$\begin{aligned}\dot{x}(t)&=\sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}\left[A_{il}x(t)+B_{1il}w_i+B_{2il}K_{ir}x(t)\right]\\ z(t)&=\sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}\left(C_{il}+D_{il}K_{ir}\right)x(t)\end{aligned} \tag{6}$$

Lemma 1. Let $a_{ij_i}\,(1\le i\le m, 1\le j_i\le N_i)$ be a set of constants satisfying

$$\sum_{i=1}^{m}a_{ij_i}<0,\ \forall 1\le j_i\le N_i\ .$$

Then, there exists at least one i such that

$$a_{ij_i}<0,\ 1\le j_i\le N_i\,.$$

Proof. It is trivial hence omitted.

Theorem 1. Let a constant $\gamma>0$ be given. Suppose there exist a positive definite matrix P and constant $\lambda_{ij_i}>0\ \ (i=1,2\cdots m,\ j_i=1,2\cdots N_i)$ such that

$$\sum_{i=1}^{m}\lambda_{ij_i}\begin{bmatrix}(A_{ij_i}+B_{2ij_i}K_{i\vartheta_i})^T P+P(A_{ij_i}+B_{2ij_i}K_{i\vartheta_i})+\\ \frac{1}{\gamma^2}PB_{1ij_i}B_{1i\vartheta_i}^T P+(C_{ij_i}+D_{ij_i}K_{i\vartheta_i})^T\bullet\\ (C_{ip_i}+D_{ip_i}K_{iq_i})\end{bmatrix}<0$$
$$i=1,2,\cdots,m,\ \ j_i,\vartheta_i,p_i,q_i=1,2,\cdots,N_i\,. \tag{7}$$

Then the state feedback controllers (5) and the following switching law (8) solve the investigated H_∞ control problem:

$$\sigma(x)=\arg\min\{\bar{V}_i(x)\overset{\Delta}{=}\max_{j_i,\vartheta_i,p_i,q_i}\{$$
$$x^T\begin{bmatrix}(A_{ij_i}+B_{2ij_i}K_{i\vartheta_i})^T P+P(A_{ij_i}+B_{2ij_i}K_{i\vartheta_i})+\\ \frac{1}{\gamma^2}PB_{1ij_i}B_{1i\vartheta_i}^T P+(C_{ij_i}+D_{ij_i}K_{i\vartheta_i})^T\bullet\\ (C_{ip_i}+D_{ip_i}K_{iq_i})\end{bmatrix}x<0,$$
$$j_i,\vartheta_i,p_i,q_i=1,2,\cdots,N_i\}\}. \tag{8}$$

Proof. From (7) we know that for any $x\neq 0$, it holds true

$$\sum_{i=1}^{m}\lambda_{ij_i}x^T\begin{bmatrix}(A_{ij_i}+B_{2ij_i}K_{i\vartheta_i})^T P+P(A_{ij_i}+B_{2ij_i}K_{i\vartheta_i})+\\ \frac{1}{\gamma^2}PB_{1ij_i}B_{1i\vartheta_i}^T P+(C_{ij_i}+D_{ij_i}K_{i\vartheta_i})^T\bullet\\ (C_{ip_i}+D_{ip_i}K_{iq_i})\end{bmatrix}x<0,$$
$$i=1,2,\cdots,m,\quad j_i,\vartheta_i,p_i,q_i=1,2,\cdots,N_i. \tag{9}$$

Notice that (9) holds for any

$j_i,\vartheta_i,p_i,q_i\in\{1,2,\cdots N_i\}$ and $\lambda_{ij_i}>0$.

The Lemma 1 guarantees that there exists at least an i such that for any j_i,ϑ_i,p_i,q_i

$$x^T\begin{bmatrix}(A_{ij_i}+B_{2ij_i}K_{i\vartheta_i})^T P+P(A_{ij_i}+B_{2ij_i}K_{i\vartheta_i})+\\ \frac{1}{\gamma^2}PB_{1ij_i}B_{1i\vartheta_i}^T P+(C_{ij_i}+D_{ij_i}K_{i\vartheta_i})^T\bullet\\ (C_{ip_i}+D_{ip_i}K_{iq_i})\end{bmatrix}x<0 \tag{10}$$

Thus, the switching law defined by (10) is well-defined.

Next, as in [20, 23], let now calculate the time derivative of Lyapunov candidate function $V(x(t)) = x^T(t)Px(t)$:

$$\dot{V} = \dot{x}^T Px + x^T P\dot{x} =$$
$$= \sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}\left(A_{il}x + B_{1il}w_i + B_{2il}K_{ir}x\right)^T Px +$$
$$+ \sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}x^T P\left(A_{il}x + B_{1il}w_i + B_{2il}K_{ir}x\right) =$$
$$= \sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}x^T\begin{bmatrix}\left(A_{il}+B_{2il}K_{ir}\right)^T P + P\left(A_{il}+B_{2il}K_{ir}\right) + \\ \frac{1}{\gamma^2}PB_{1il}B_{1ir}^T P + \sum_{s=1}^{N_i}\eta_{is}\sum_{d=1}^{N_i}\eta_{id} \\ \left(C_{il}+D_{il}K_{ir}\right)^T\left(C_{is}+D_{is}K_{id}\right)\end{bmatrix}x +$$
$$+\sum_{l=1}^{N_i}\eta_{il}\left(w_i^T B_{1il}^T Px + x^T PB_{1il}w_i\right) -$$
$$-\sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}x^T\begin{bmatrix}\frac{1}{\gamma^2}PB_{1il}B_{1ir}^T P + \sum_{s=1}^{N_i}\eta_{is}\sum_{d=1}^{N_i}\eta_{id} \\ \left(C_{il}+D_{il}K_{ir}\right)^T\left(C_{is}+D_{is}K_{id}\right)\end{bmatrix}x \tag{11}$$

The second term on the right-hand side of (11) is found:

$$\sum_{l=1}^{N_i}\eta_{il}\left(w_i^T B_{1il}^T Px + x^T PB_{1il}w_i\right) =$$
$$w_i^T\left(\sum_{l=1}^{N_i}\eta_{il}B_{1il}^T Px\right) + \left(\sum_{l=1}^{N_i}\eta_{il}B_{1il}^T Px\right)^T w_i \tag{12}$$

The last term on the right-hand of (11) is found:

$$\sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}x^T\begin{bmatrix}\frac{1}{\gamma^2}PB_{1il}B_{1ir}^T P + \sum_{s=1}^{N_i}\eta_{is}\sum_{d=1}^{N_i}\eta_{id} \\ \left(C_{il}+D_{il}K_{ir}\right)^T\left(C_{is}+D_{is}K_{id}\right)\end{bmatrix}x =$$
$$\left(\frac{1}{\gamma}\sum_{l=1}^{N_i}\eta_{il}B_{1il}^T Px\right)^T\left(\frac{1}{\gamma}\sum_{r=1}^{N_i}\eta_{ir}B_{1ir}^T Px\right) +$$
$$\left[\sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}\left(C_{il}+D_{il}K_{ir}\right)x\right]^T\left[\sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}\left(C_{il}+D_{il}K_{ir}\right)x\right] \tag{13}$$

By virtue of (10), it follows:

$$x^T\left[\left(A_{ij_i}+B_{2ij_i}K_{i\vartheta_i}\right)^T P + P\left(A_{ij_i}+B_{2ij_i}K_{i\vartheta_i}\right)\right]x \le$$
$$x^T\begin{bmatrix}\left(A_{ij_i}+B_{2ij_i}K_{i\vartheta_i}\right)^T P + P\left(A_{ij_i}+B_{2ij_i}K_{i\vartheta_i}\right) + \\ \frac{1}{\gamma^2}PB_{1ij_i}B_{1i\vartheta_i}^T P + \left(C_{ij_i}+D_{ij_i}K_{i\vartheta_i}\right)^T \bullet \\ \left(C_{ip_i}+D_{ip_i}K_{iq_i}\right)\end{bmatrix}x < 0$$
$$j_i, \vartheta_i, p_i, q_i = 1,2,\cdots,N_i. \tag{14}$$

When $w_i = 0$, by virtue of relationships (4 a, b, c), due to (11) and (14), one can calculate:

$$\dot{V} = \sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}x^T\left[\left(A_{il}+B_{2il}K_{ir}\right)^T P + P\left(A_{il}+B_{2il}K_{ir}\right)\right]x < 0. \tag{15}$$

Thus, the system (1) in the closed loop and under controls (5) is asymptotically stable.

Combing (11), (12) and (13) gives rise to

$$\dot{V} \le \sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}\sum_{s=1}^{N_i}\eta_{is}\sum_{d=1}^{N_i}\eta_{id}x^T Q_{ilrsd}x - z^T z + \gamma^2 w_i^T w_i -$$
$$\left(\gamma w_i - \frac{1}{\gamma}\sum_{l=1}^{N_i}\eta_{il}B_{1il}^T Px\right)^T\left(\gamma w_i - \frac{1}{\gamma}\sum_{l=1}^{N_i}\eta_{il}B_{1il}^T Px\right) \tag{16}$$

where

$$Q_{ilrsd} = \left(A_{il}+B_{2il}K_{ir}\right)^T P + P\left(A_{il}+B_{2il}K_{ir}\right) +$$
$$\frac{1}{\gamma^2}PB_{1il}B_{1ir}^T P + \left(C_{il}+D_{il}K_{ir}\right)^T\left(C_{is}+D_{is}K_{id}\right)$$

Without loss of generality, let suppose zero initial state $x(0) = 0$ and Lyapunov function value $V(x(0)) = 0$ at the initial state [20, 23]. Now, by re-arranging (16) and then solving the integral in it for t from 0 to ∞, one can calculate the following inequality yield:

$$\|z(t)\|_2^2 \le \|z(t)\|_2^2 - \lambda_{\max}\left(\sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}\sum_{s=1}^{N_i}\eta_{is}\sum_{d=1}^{N_i}\eta_{id}Q_{ilrsd}\right)\|x(t)\|_2^2 +$$
$$+V(\infty) + \gamma^2\left\|w_i(t) - \frac{1}{\gamma^2}\sum_{l=1}^{N_i}\eta_{il}B_{1il}^T Px\right\|_2^2 \le \gamma^2\|w_i(t)\|_2^2$$

where

$$\lambda_{\max}\left(\sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}\sum_{s=1}^{N_i}\eta_{is}\sum_{d=1}^{N_i}\eta_{id}Q_{ilrsd}\right)$$

denotes the maximal eigenvalue of matrix

$$\sum_{l=1}^{N_i}\eta_{il}\sum_{r=1}^{N_i}\eta_{ir}\sum_{s=1}^{N_i}\eta_{is}\sum_{d=1}^{N_i}\eta_{id}Q_{ilrsd}.$$

In addition, it should be noted that in the above derivations to establish results confirming system stability analysis [20] the well-known Schur Complement Lemma and Uncertainty Representation Lemma for specific symmetric matrices, in from literature [21–22] play important role of crucial tools. Both these lemmas are recalled below in here.

Lemma 2. (Schur Complement). For a given the symmetric

$$M=\begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix},$$

where M_{11} and M_{21} are symmetric matrices, the following inequality condition statements are equivalent:

1/. $M<0$,

2/. $M_{11}<0,\ M_{22}-M_{21}M_{11}^{-1}M_{12}<0$,

3/. $M_{22}<0,\ M_{11}-M_{12}M_{22}^{-1}M_{21}<0$.

Lemma 3. Assume the uncertainty $F(t)$ and matrices L, $M=M^T$, S, and N of appropriate dimensions. Then the following two condition statements are equivalent:

1/. $M+SF(t)N+S^TF^T(t)N^T<0$,

2/. For $\rho>0$ an existing deterministic or stochastic real-number it holds true

$$M=\begin{bmatrix} M & \rho S & N^T \\ \rho S^T & -\rho I & \rho L^T \\ N & \rho L & -\rho I \end{bmatrix}<0.$$

4. ILLUSTRATIVE EXAMPLE

In order to illustrate the just presented design analysis approach let consider its application to the stability control of problem of a room air regulating system [8, 19]. The state equation of the plant system is given as follows:

$$\ddot{T}_n=-(\frac{1}{T_1}+\frac{1}{T_2})\dot{T}_n-\frac{1}{T_1T_2}T_n+\frac{k_1k_2}{T_1T_2}u$$

In here quantities denote: T_n is the air temperature variable in air-conditioned room [℃]; $\dot{T}_n$ is the rate of air temperature variable of the air-conditioned room [℃/min]; T_1 is the empiric inertia time constant of the air-conditioned room [min]; k_1 is the amplifying coefficient (gain) of the room equilibrium constant temperature [℃/℃]; T_2 is the empiric inertia time constant of the steam heater [min]; k_2 is the gain coefficient of the electric heating actuator [℃/℃]; and u is the control input variable in terms of electrical power. The reported empirically found time constants are as follows:

*When room temperature is considered lower than human comfort sensing, $T_1=20.30$ min, $T_2=1$ min.

**When room temperature is considered higher than human comfort sensing, $T_1=30.40$ min, $T_2=2.5$ min.

In order to illustrate the stability control design analysis of this system, coordinate transformation is carried out so as to transform the problem into zero-state stability control. Taking into consideration the available redundancy of circuit actuator the common sense fuzzy model is converted into the switched fuzzy model to advance arriving at scheduled temperature rise speed of air regulating system operation. Therefore the dynamics of the considered air regulating system operation is approximate by the following *T-S* fuzzy rule based model:

R_1^1: if x_1 is P_{11}^1, *close to positive,* then

$$\dot{x}=A_{11}x+B_{111}w_1+B_{211}u_1,\ z=C_{11}x+D_{11}u_1,$$

R_1^2 : if x_1 is N_{11}^2, *close to negative,* then

$$\dot{x}=A_{12}x+B_{112}w_1+B_{212}u_1,\ z=C_{12}x+D_{12}u_1,$$

R_2^1: if x_1 is P_{21}^1 ,*close to positive,* then

$$\dot{x}(t)=A_{21}x+B_{121}w_2+B_{221}u_2,\ z=C_{21}x+D_{21}u_2,$$

R_2^2: if x_1 is N_{21}^2, *close to negative,* then

$$\dot{x}(t)=A_{22}x+B_{122}w_2+B_{222}u_2,\ z=C_{22}x+D_{22}u_2,$$

where:

$$A_{11}=\begin{bmatrix} -0.5 & 4 \\ -0.943 & -1.0493 \end{bmatrix},$$

$$A_{12} = \begin{bmatrix} -0.5 & 3 \\ -0.132 & -0.4529 \end{bmatrix}$$

$$B_{111} = B_{112} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, B_{211} = \begin{bmatrix} 0 \\ 0.4926 \end{bmatrix},$$

$$B_{212} = \begin{bmatrix} 0 \\ 0.1316 \end{bmatrix},$$

$$A_{21} = \begin{bmatrix} 1 & 2 \\ -0.2941 & -1.4321 \end{bmatrix},$$

$$A_{21} = \begin{bmatrix} 1 & 2 \\ -0.4706 & -0.7535 \end{bmatrix},$$

$$B_{121} = B_{122} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, B_{221} = \begin{bmatrix} 0 \\ 0.5765 \end{bmatrix},$$

$$B_{222} = \begin{bmatrix} 0 \\ 0.1765 \end{bmatrix},$$

$$C_{11} = C_{12} = \begin{bmatrix} 1 & 1 \end{bmatrix},\ C_{21} = C_{22} = \begin{bmatrix} 1 & 0 \end{bmatrix},$$

$$D_{11} = D_{12} = 0.03,\ D_{21} = D_{22} = 0.04.$$

The issue of defining appropriate membership functions as pointed out by Lotfi A. Zadeh [25], the founder and inventor of fuzzy logic and fuzzy systems [25], is essentially an application dependent problem. Because it is dependent on the universe of discourse set (i.e. physical nature of plan's state space) hence it is open to exploration within the context of the given case study application. This issue was thoroughly explored in the studies [8, 19], and concluded that fuzzy-set membership functions defined below have wide applicability and usually are optimum statedependent ones:

$$\mu_{P_{11}^1}(x_1) = \mu_{P_{21}^1}(x_1) = 1 - \frac{1}{1+e^{-2x_1}},$$

$$\mu_{N_{11}^2}(x_1) = \mu_{N_{21}^2}(x_1) = \frac{1}{1+e^{-2x_1}}.$$

Further, let explore the considerable case with robustness index level $\gamma = 1$. Then, due to the derived state-feedback control formula:

$$u_i(t) = \sum_{l=1}^{N_i} \eta_{il} K_{il} x(t),\ i = 1,2,$$

the inequality of Theorem 1 is subject to evaluating calculation of the following matrix inequality:

$$\sum_{i=1}^{2} \lambda_{ij_i} \begin{bmatrix} (A_{ij_i} + B_{2ij_i} K_{i\vartheta_i})^T P + P(A_{ij_i} + B_{2ij_i} K_{i\vartheta_i}) + \\ \frac{1}{\gamma^2} P B_{1ij_i} B_{1i\vartheta_i}^T P + (C_{ij_i} + D_{ij_i} K_{i\vartheta_i})^T \bullet \\ (C_{ip_i} + D_{ip_i} K_{iq_i}) \end{bmatrix} < 0$$
$$i = 1,2, \quad j_i, \vartheta_i, p_i, q_i = 1,2,\cdots,N_i. \qquad (17)$$

Without loss of generality let further be assumed simple and uniform values $\lambda_{ij_i} = 1$, because these are out of the matrix inequality.

According to Schur Complement Lemma [21–23], matrix inequalities (17) can be turned into the solvable LMI and, if needed to involve some uncertainty factor, further alyzed by using Uncertainty Representation Lemma. Then the solution for gain matrices are computed with the LMI toolbox as follows:

$$K_{11} = [-0.131 \quad -0.1148],$$
$$K_{12} = [-0.0623 \quad -2.302],$$

$$K_{21} = [-4.4991 \quad -2.4986],$$
$$K_{22} = [-5.4991 \quad -3.4986],$$

$$P = \begin{bmatrix} 0.0937 & 0.2146 \\ 0.2146 & 0.6417 \end{bmatrix}.$$

The design the switching law

$$\sigma(x) = \arg\min\{\overline{V}_i(x)\},$$

as emphasized in Theorem 1, in this example was emulated by means of the following formula:

$$\sigma(x) = \arg\min\{\overline{V}_i(x)\} \stackrel{\Delta}{=} \max_{j_i,\vartheta_i,p_i,q_i} \{$$
$$x^T \begin{bmatrix} (A_{ij_i} + B_{2ij_i} K_{i\vartheta_i})^T P + P(A_{ij_i} + B_{2ij_i} K_{i\vartheta_i}) + \\ \frac{1}{\gamma^2} P B_{1ij_i} B_{1i\vartheta_i}^T P + (C_{ij_i} + D_{ij_i} K_{i\vartheta_i})^T \bullet \\ (C_{ip_i} + D_{ip_i} K_{iq_i}) \end{bmatrix} x < 0$$
$$j_i, \vartheta_i, p_i, q_i = 1,2\}\}. \qquad (18)$$

A selected set of graphically depicted simulation results using Matlab-Simulink platform [34–37] are presented in the sequel in order to demonstrate both the acting feasibility and achievable performance by the proposed control design synthesis in the closed loop. The simulation results are

obtained by assuming plant system is at initial disturbed states to cold/chilly temperatures $[-3 \quad 0]^T$.

Time evolutions of the system states of this two-subsystem, two-dimensional system plant in four-rule Takagi-Sugeno representation model the closed loop with initial conditions $[-3 \quad 0]^T$ and under the hybrid control law of the H_∞ control and switching based control (Lemma 1 and Theorem 1) are presented in Figure 1. Similarly the time-evolution of the effective acting switching time sequence is presented in Figure 2.

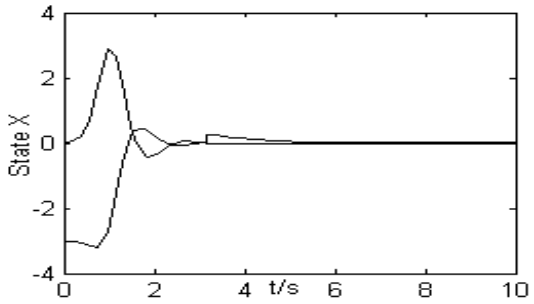


Fig. 1. The state response of the system with constructed overall PDC controller (5a)–(5b) according to Theorem 1 under switching law (8)

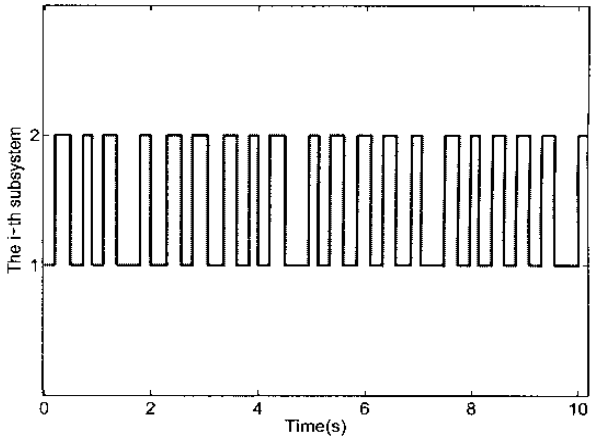


Fig. 2. The switching time sequence (8) that accompany the constructed PDC controller (5a)–(5b) according to Theorem 1

It should be noted, by the time $t = 10$ s, switching sequence exhibits almost periodically repeated switching jumps. Apparently, the state feedback H_∞ robust control problem with $\gamma = 1$ guarantying asymptotic stability is solved and the respetive two controls are depicted in Figure 3. Furthermore, in this particular plant example, it is interesting to notice that as if from the time $t = 10$ s onwards there appeared no more effective need for controlling actions.

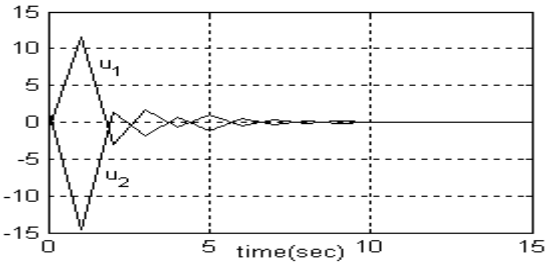


Fig. 3. The H_∞ state-feedback controls (5b) that accompany the constructed controller in PDC-architecture (5a) according to Theorem 1, and switching law (8); no further controlling activities are noticeable beyond 10 s whereas rather strong are during the first few seconds

Practically the equilibrium operating rise of controlled room temperature to the equilibrium state is achieved in finite time.

It is also interesting to note, in this traditional temperature control system but employing the hybrid H_∞ plus switching sequence in PDC-architecture of fuzzy-logic driven control certain additionnal highlights are obtained when subject to unknown impulsive Markov stochastic sudden disturbance hits on the actuators over longer period of operating time. At this point let recall the introduced Uncertainty Representation Lemma in the previous section. The found simulation results for feasible acting controls and achievable controlled states are depicted in Figures 4 and 5, respectively.

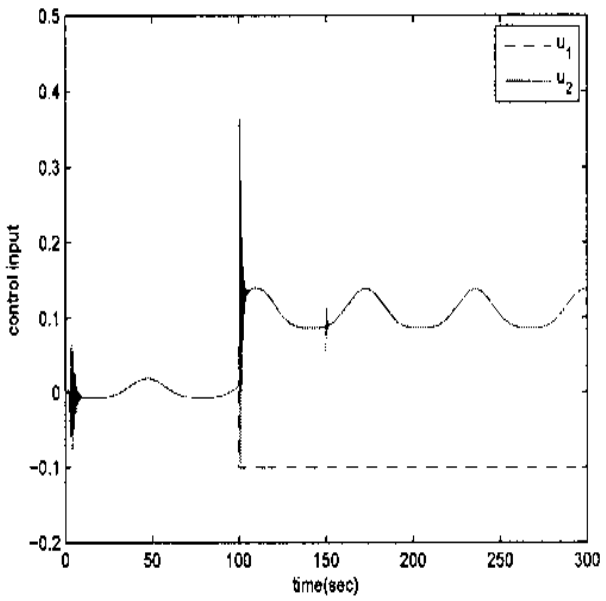


Fig. 4. Time history of the controlling activities under employing the proposed hybrid H_∞ plus switching sequence in PDC-architecture of fuzzy-logic driven control during a long operating time when it is being disturbed by sudden unknown Markov impulsive hits on actuating heaters

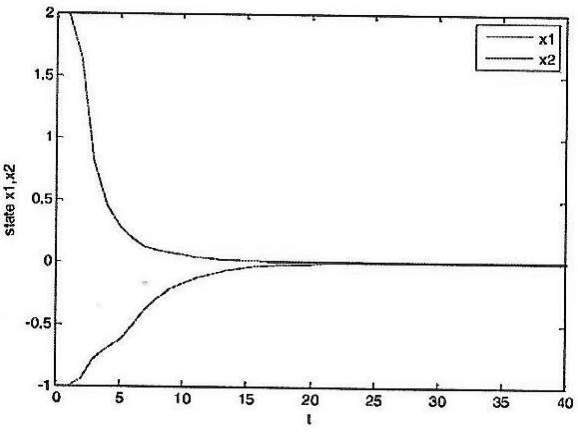


Fig. 5. Time history during the first 40 seconds of the controlled temperature state following Markov impulsive disturbance hits on actuating heaters; this same pattern repeats almost periodically following the operating controls.

5. CONCLUSION

The problem of state feedback H_∞ control for switched fuzzy systems is investigated via a non-traditional approach. In particular, considerable attention is focused on exploring switched fuzzy model involving implicit context of reliability, which has not been considered in previous studies even in context of reliable controls. The state space $\Omega \subseteq R^n$ of a switched system observed as a (fuzzy-)set partition $\Omega \subseteq \{\Omega_1, \cdots, \Omega_i, \cdots, \Omega_m\}$ into m sub-areas, thus every subarea emulating one switched subsystem. The orchestrated switching among subsystems via a purpose driven switching law design is aimed at ensuring stability of the overall switched system.

On the grounds of envisaged switching strategy, feedback controller and switching law of the state-dependent form are developed such that the problem of H_∞ control is solved. Sufficient condition for asymptotic stability based on Lyapunov theory is given. According to this condition, in order to check closed-loop stability a certain convex combination of subsystem matrices is to be checked, which is fairly easy. Simulation results for an application to real-world room air-conditioning illustrate both the effectiveness and feasible quality operating performance of this control design synthesis.

Acknowledgements: The authors acknowledge with gratitude the contributions made in due times by the respective doctoral students at Northeastern University of Shenyang in Shenyang, College of Information Science and Engineering, Liaoning, P. R. of China, at SS Cyril & Methodius University in Skopje, Faculty of Electrical Engineering & Information Technologies, N. Macedonia, with whom they have accomplished all research endeavors during last twenty years, this study inclusive.

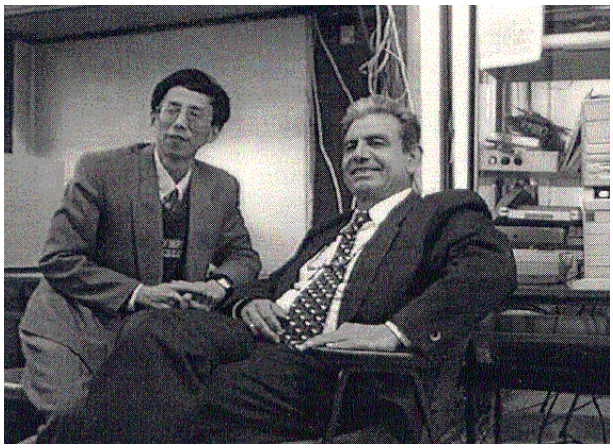


Fig. 6. December 1996 in FEIT Laboratory of Electronics: Days 1996-97 at IASE-FEIT of fruitful postdoctoral research and visiting professorship by Yuan-Wei Jing (Systems & Control Theory to our students) in collaboration with Georgi Dimirovski

REFERENCES

[1] Zhao, J., Dimirovski, G. M. (2004): Quadratic stability for a class of switched nonlinear systems. *IEEE Transactions on Automatic Control*, vol. **49**, no. 4, pp. 574–578.

[2] Ooba, *T*., Funahashi, Y. (1997): On a common quadratic Lyapunov functions for widely distant systems. *IEEE Transactions on Automatic Control*, vol. **42**, no. 12, pp. 1697–1699.

[3] Branicky, M. S. (1998.): Multiple Lyapunov functions and other analysis tools for switched and hybrid systems. *IEEE Transactions on Automatic Control*, vol. **43**, no. 4, pp. 475–482.

[4] Branicky, M. S. (1994): Stability of switched and hybrid systems. In: *Proceedings of the IEEE Conference on Decision and Control, Lake Buena Vista, FL*, IEEE, pp. 3498–3503.

[5] Gollu, A., Varaiya P. P. (1989): Hybrid dynamical system. In: *Proceedings of the IEEE Conference on Decision and Control, Tampa, FL*, IEEE, pp. 2708–2712.

[6] Jeon. D., Tomizuka, M. (1993): Learning hybrid force and position control of robot manipulators. *IEEE Transactions on Automat. Control*, vol. **39**, no. 4, pp. 423–431.

[7] Zhao, J., Spong, M. W. (2001): Hybrid control for global stabilization of the cart-pendulum system. *Automatica*, vol. **37**, no. 12, pp. 1941–1951.

[8] Tanaka, K., Wang, H. O. (2001): *Fuzzy Control Systems Design and Analysis: A Linear Matrix Inequality Approach*. J. Wiley & Sons, New York, NY.

[9] Lee, K., Jeung, E., Park, H. (2001): Robust fuzzy H∞ control of uncertain nonlinear systems via state feedback: an LMI approach. *Fuzzy Sets and Systems*, vol. **120**, pp. 123–134.

[10] Feng, G., Ma, J. (2001): Quadratic stabilization of uncertain discrete-time fuzzy dynamic systems. *IEEE Transactions on Circuits and Systems I*: *Fundamental Theory and Applications*, vol. **48**, pp.1337–1344.

[11] Cao, Y. Y., Frank, P. M. (2001): Stability analysis and synthesis of nonlinear time-delay systems via linear Takagi-Sugeno fuzzy models. *Fuzzy Sets and Systems*, vol. **124**, no. 2, pp. 213–229.

[12] Chen, B. S., Tseng, C. S., Uang, H. J. (2000): Mixed H_2/H_∞ fuzzy output feedback control design for nonlinear dynamic systems: an LMI approach. *IEEE Trans. on Fuzzy Systems*, vol. **8**, pp. 249–265.

[13] Palm, R., Driankov, D. (1998): Fuzzy switched hybrid systems – modeling and identification. In: *Proceedings of the 1998 IEEE ISIC/CIRA/ISAS Joint Conference, Gaithersburg, VA.* The IEEE, Piscataway, NJ, pp. 130–135.

[14] Tanaka, K., Iwasaki, M., Wang, H. O. (2000): Stability and smoothness conditions for switching fuzzy systems. In: *Proceedings of the American Control Conference, Chicago, IL,* The IEEE, Piscataway, NJ, pp. 2475–2478.

[15] Tanaka, K., Iwasaki, M., Wang, H. O. (2001): Switching control of an R/C hovercraft: stabilization and smooth switching. *IEEE Transactions on Systems, Man, and Cybernetics*, vol. **31**, no. 6, pp. 853–863.

[16] Hiroshi, O., Tanaka, K., Wang, H. O. (2003): Switching fuzzy control for nonlinear systems. In: *Proceedings of the 2003 IEEE International Symposium on Intelligent Control, Houston, TX*. The IEEE, Piscataway, NJ, pp. 281–286.

[17]. Choi, D. J, Park, P. (2002): State-feedback H∞ controller design for discrete–time switching fuzzy systems. In: *Proceedings of the 41st IEEE Conference on Decision and Control, Las Vegas,* NE. The IEEE, Piscataway, NJ, pp. 191–196.

[18] Choi, D. J., Park, P. (2004): Guaranteed cost controller design for discrete-time switching fuzzy systems. *IEEE Transactions on Systems, Man, and Cybernetic*s, vol. **34**, no. 1, pp. 110–119.

[19] He, X. Q. (2000): *Stability and application of a class of multiple variables fuzzy systems*. PhD dissertation, Northeastern University, Shenyang, Liaoning, P. R. of China.

[20] Barnett, S., Storey, C. (1970): *Matrix Method in Stability Theory*. Nelson, London, UK.

[21] Bellman, R. (1970): *Introduction to Matrix Analysis* (2nd edition). McGraw-Hill, New York, NY.

[22] Boyd, S., Ghaoui, L. E., Feron. E., Balakrishnan, V. (1994): *Linear Matrix Inequalities in Systems and Control Theory*. The SIAM, Philadelphia, PA.

[23] Liberzon, D. (2003): *Switching in System and Control*. Birkhauser, Boston, MA.

[24] Zadeh, L. A. (1980): Inference in fuzzy logic. *The IEEE Proceedings*, vol. **68**, pp. 124–131.

[25] Zadeh, L. A. (2008): Is there a need for fuzzy logic? *Information Sciences*, vol. **178**, pp. 2751–2779.

[26] Yang, H., Dimirovski, G. M., Zhao, J. (2008): Switched fuzzy systems: representation modeling, stability and control design. In: J. Kacprzyk, Editor-in-Chief, *Studies in Computational Intelligence 109 – Intelligent Techniques and Tool for Novel System Architectures*. Springer-Verlag, Berlin – Heidelberg, DE, pp. 169–184.

[27] Ojleska, V. M., Kolemiševska-Gugulovska, T., Dimirovski, G. M. (2010): Influence of the state space partitioning into regions when designing switched fuzzy controllers. *Facta Universitatis, Series Automatic Control and Robotics*, vol. **9**, no. 1, pp. 103–112.

[28] Ma, R., Zhao, J., Dimirovski, G. M. (2013): Backstepping robust Hinf control design for a class of uncertain switched nonlinear systems under arbitrary switching. *Asian Journal of Control*, vol. **15**, no. 1, pp. 1–10.

[29] Huo, B. Y., Xia, Y. Q., Lu, K. F., Fu, M. Y. (2015): Adaptive fuzzy finite-time fault-tolerant attitude control for rigid spacecraft. *Journal of the Franklin Institute*, vol. **352**, no. 10, pp. 4225–4246.

[30] Wang, J., Hu, Zh., Yue, H., Dimirovski, G. M. (2017): Restricted finite-time control for nonlinear systems. *Journal of Systems Science & Mathematical Sciences*, vol. **37**, no. 4, pp. 1–8.

[31] Zhang, D., Jing, Y., Zhang, Q., Dimirovski, G. M. (2020): Stabilization od singular T-S fuzzy Markovian jump systems with mode-dependent derivative-term coefficient via sliding mode control. *Applied Mathematics & Computation*, vol. **364**, art. 124643 (1–19).

[32] Gao, S., Jing, Y., Dimirovski, G. M., Zheng, Y. (2021): Adaptive fuzzy fault-tolerant control for the attitude tracking of spacecraft within finite time. *Acta Astronautica*, vol. **180**, pp. 166–180.

[33] Shen, J., Jing, Y., Dimirovski, G. M. (2022): Fixed-time congestion tracking for a class of uncertain TPC/AQM computer and communication networks. *International Journal of Control, Automation & Systems*, vol. **20**, is. 3, pp. 758–768.

[34] Gahinet, P., Nemirovski, A., Laub, A. J., Chilali, M. (1995): *LMI Control Toolbox*. The Mathworks, Natick, NJ.

[35] MathWorks (1995): *LMI Toolbox*. The MathWorks, Inc. Natick, NJ:

[36] MathWorks (1992)*: Matlab Simulink* – Version 5. The Mathworks Inc. Natick, NJ.

[37] MathWorks (1995): *Fuzzy Toolbox*. The Mathworks Inc. Natick, NJ,

Journal of Electrical Engineering and Information Technologies, Vol. **7,** No. 2, pp. 97–100 (2022)
Article 200
In print: ISSN 2545–4250
Received: November 7, 2022
On line: ISSN 2545–4269
Accepted: November 21, 2022
UDC: 621.395.623.7.049.7
DOI: https://doi.org/10.51466/JEEIT2272200097f

Original scientific paper

OPTIMAL DESIGN FOR AN ON-WALL MOUNTED LOUDSPEAKER

Vladimir Filevski

AUDIO EXPERT DOOEL,
Kozle 3, No. 6, Skopje, Republic of North Macedonia
vfilevski@yahoo.com

A b s t r a c t: This paper describes the problem arising from mounting the loudspeaker on a wall, which results in an uneven frequency response. The problem arises from the destructive interference of the direct sound wave emitted by the loudspeaker and the reflected sound wave from the wall. Examples are given of two known solutions for commercial loudspeakers that made certain improvement in view of the mentioned problem, followed by a new proposal for a solution of the same problem.

Key words: loudspeaker; wall-mounted; on-wall

ОПТИМАЛНА КОНСТРУКЦИЈА НА ЗВУЧНИК НАМЕНЕТ ЗА МОНТИРАЊЕ НА ѕИД

А п с т р а к т: Во овој труд е опишан проблемот што произлегува од монтирањето на кутијата на звучниот систем на ѕид, што се манифестира како нерамна амплитудно-фреквенциска карактеристика. Проблемот произлегува од деструктивната интерференција на директниот звучен бран емитиран од звучникот и од ѕидот рефлектираниот звучен бран. Дадени се примери на две познати решенија на комерцијални звучници што дале одредено подобрување на спомнатиот проблем, а во продолжение е прикажан и еден нов предлог за решение на проблемот.

Клучни зборови: зучник монтиран на ѕид

INTRODUCTION

As a rule, loudspeakers are mounted on some distance from the wall behind them. But, because of lack of space, sometimes this is not possible, so loudspeakers have to be mounted directly on the wall, leaving at the most 10 cm to 30 cm distance from the front panel of the loudspeaker cabinet to the back wall, that is with most of the small to medium size loudspeakers.

Figure 1 shows measured frequency response of a small loudspeaker with a 13 cm mid-bass unit, mounted on a front panel with a width of 16 cm. The distance between the front surface of the front panel and the back surface of the back panel is 21 cm. The measured frequency response of the mid-bass is typical for loudspeaker units this small and its frequency range is up to 5 kHz, so that in order to cover the whole audio spectrum up to 20 kHz a tweeter that usually works above 2,5 kHz via appropriate crossover should be used.

When the loudspeaker from Figure 1 is mounted on wall with its front panel on a 21 cm distance from the wall, we get what is described on Figure 2.

We can see on Figure 2 that the difference between the paths of the reflected and the direct soundwave is L2 + L3, which results in partial cancellation of the soundwave at the measuring point (the microphone) in the vicinity of the frequency which

is one half of the wave length: $2f = c/(L1 + L2)$, where c is the speed of the sound in the air. The cancellation is shown on Figure 3 as a deep in measured frequency response in the vicinity of f = 345 Hz, with the same loudspeaker as on Figure 1, mounted on the wall as on Figure 2.

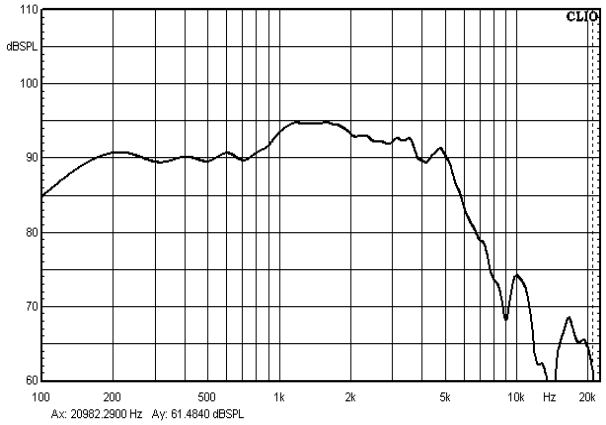


Fig. 1. Measured frequency response of a small loudspeaker, in free space, with no reflections

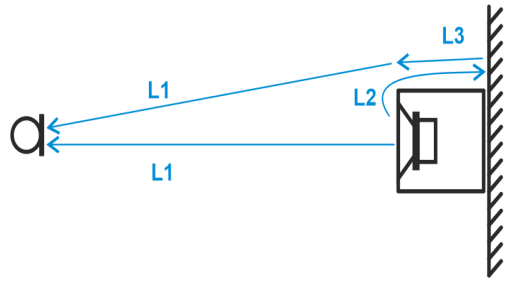


Fig. 2. Propagation of sound waves emitted from a loudspeaker mounted directly on a wall: direct sound wave (L1, below) and reflected sound wave (L2 + L3 + L1, above) from the wall

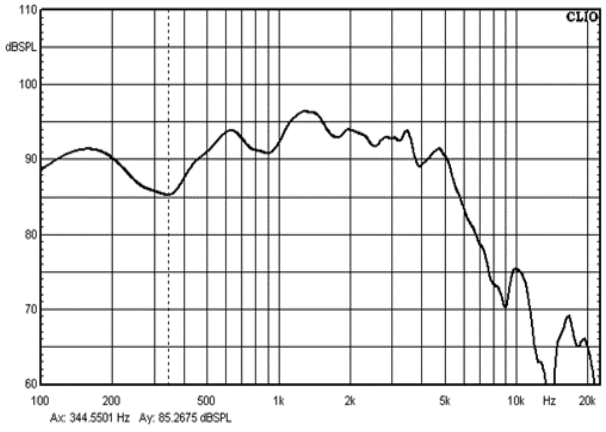


Fig. 3. Measured frequency response with loudspeaker mounted directly on wall, with the reflection from the back wall included

It should be emphasized that this cancellation appears only when measuring the direct sound signal and the one reflected from the wall, excluding any reflection from the rest of the walls in the room (as well as other bigger objects inside the room, e.g. the furniture). In real situation, when all the reflections in the room are included, the cancellation may not be that much pronounced, but it is still there. At lower frequencies (especially below 150 Hz) the difference between the paths of the direct and reflected sound is very small part of the wave length, so that the direct and the reflected sound are practically in phase, which results in amplifying of the lowest frequencies, in ideal situation up to 6 dB.

REVIEW OF THE KNOWN SOLUTION

The problem with cancellation of the direct sound wave and the one reflected from the wall on which the loudspeaker is mounted has been researched in the literature [1], where stated are two solutions that lead to flatter frequency response (especially in the low frequency range), the first one being offered the same year (1974) as commercial product – Figure 4.

The first solution (from Figure 4.) is schematically presented on Figure 5.

Fig. 4. Commercial loudspeaker (Allison 6) with better frequency response – the mid-bass unit is on the top panel of the loudspeaker box, the tweeter is on the front panel, both protected with a grille fabric

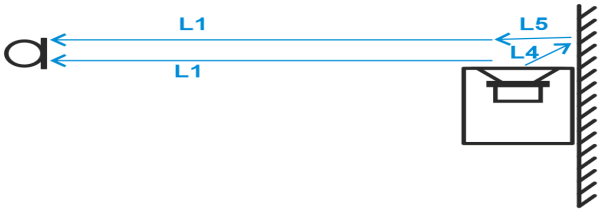


Fig. 5. Propagation of sound waves emitted from a loudspeaker mounted directly on wall, with mid-bass unit on the top panel of the loudspeaker box: direct soundwave (L1, below) and reflected soundwave (L4 + L5 + L1, above) from the wall

Figures 4 and 5 show that low frequency mid-bass unit is mounted as close to the wall as possible, which reduces the difference between the paths of the direct and the reflected sound wave L4 + L5, in relation to L2 + L3 from the previous example on Figure 2. It results in moving up of the frequency of cancellation, as seen on Figure 6.

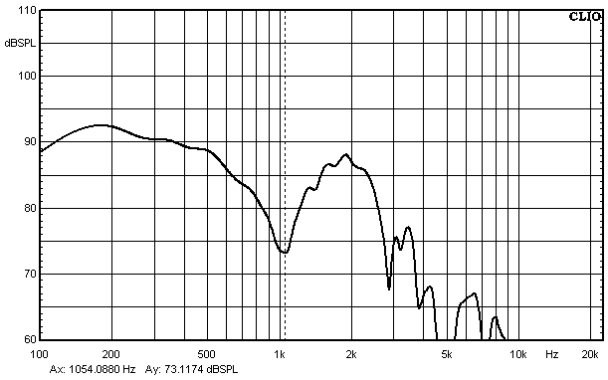


Fig. 6. Measured frequency response from a loudspeaker with a mid bass unit placed on the upper panel of the loudspeaker box very close to the wall, with frequency response only from the wall included

In reality, with all the sound reflection in the room included, this cancellation is not that deep, and not that intrusive for the ears as it happens toward higher frequencies.

Literature [1] suggests a second solution as well to achieving minimum possible difference between the paths of the direct sound wave and the one reflected from the wall – as shown on Figure 7.

Figure 7 shows that there is no reflected sound wave, because the loudspeaker unit, the panel of the loudspeaker enclosure (on which the unit is mounted) together with the wall surface form a rudiment kind of horn, through which only the direct sound wave passes. This means that there is no reflected sound wave to possibly interfere with the direct sound wave, thus no deep in the frequency response.

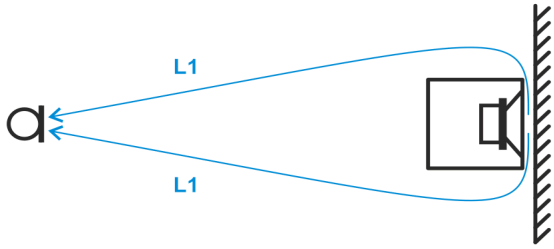


Fig. 7. Propagation of soundwaves emitted from loudspeaker mounted directly on a wall, very close to the wall (5 cm)

Figure 8 shows measured frequency response that really shows no presence of deeps, at the same time showing the effect of the horn – amplifying of part of the mid-range frequencies of around 800 Hz (which can be flatten by the crossover) as well as sudden drop of frequency response above 1200 Hz.

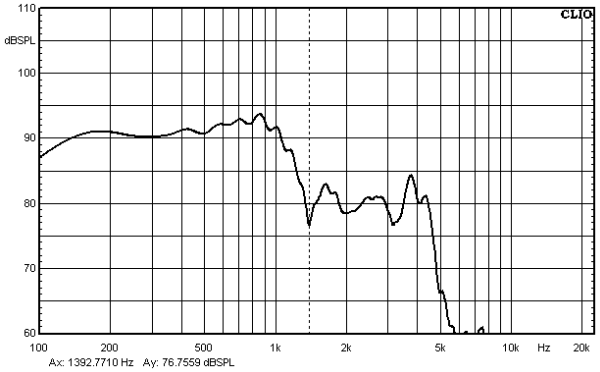


Fig. 8. Measured frequency response from a loudspeaker mounted directly toward the wall, at distance of 5 cm

The drop above 1200 Hz asks for a tweeter that can work starting from around (approximately) 1500 Hz. Crossover frequency this low can be withstand only by a high quality (expensive also) tweeter built in a horn.

There is a commercial loudspeaker of this kind on the market – Figure 9, with a crossover frequency of 1600 Hz.

Fig. 9. Commercial loudspeaker (JBL Control HST) with mid-bass unit positioned toward the wall at close distance, plus two tweeters in short horns, positioned outwards

IMPROVED CONSTRUCTION

Figure 10 shows a suggestion for an improved construction, inspired by the construction on Figure 7.

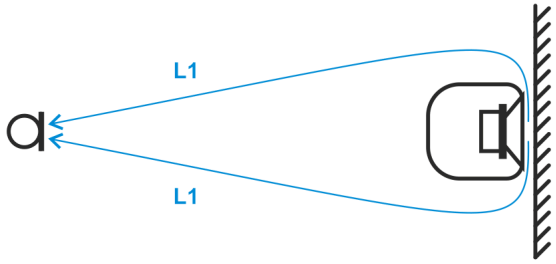


Fig. 10. Improved construction of the loudspeaker "box", with rounded edges of wide radius

The problem of the construction on Figure 7 and Figure 9 is the back panel of the box (even there is a chamfering of the left and the right vertical edge of the loudspeaker box from Figure 9) which results in uneven expansion of the horn comprising from the mid-bass unit, the panel on which it is mounted and the wall itself, so that the working range is shortened toward high frequency band. At the same time unwanted diffractions on the sharp edges of the loudspeaker box appear.Figure 11 shows measured frequency response of the prototype of the loudspeaker box, with the construction according Figure 10, only in this case the rounding of the surface is extreme – the loudspeaker "box" is actually a plastic sphere.

Figure 11 shows that the frequency response has been widen toward high frequency spectrum, thus the crossover frequency with the tweeter can be moved to comfortable 2500 Hz, easily withstood by a tweeter of an average quality. Small peaks in the vicinity of 1000 Hz and 2000 Hz can be flattened with the crossover or adequate phase plug in front of the membrane of mid-bass unit.

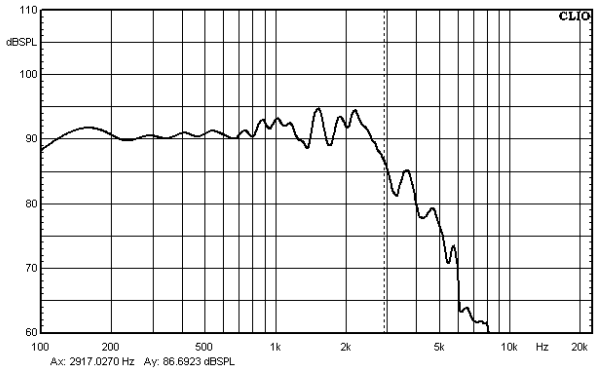


Fig. 11. Measured frequency response of improved construction

CONCLUSION

This paper analyzes the problems with the uneven frequency response inherent to all on-wall loudspeakers, presents the two known solutions and gives a suggestion for a better (improved) construtions of the loudspeaker box with wider frequency range.

Further researches should lead toward a possibly better construction of the loudspeaker box, with an accent on the most appropriate shape of the back panel as well as check for even better results by adding a phase plug in front of the membrane of the mid-bass unit.

REFERENCES

[1\] Roy, F. Allison (1974): The influence of room boundaries on loudspeaker power output, *Journal of AES*, Volume 22, Number 5, June.

Journal of Electrical Engineering and Information Technologies, Vol. **7,** No. 2, pp. 101–109 (2022)
Article 201 In print: ISSN 2545–4250
Received: November 18, 2022 On line: ISSN 2545–4269
Accepted: December 3, 2022 UDC: 006.91:621.3.03-021.423
DOI: https://doi.org/10.51466/JEEIT2272201101chb

Original scientific paper

INFRASTRUCTURE DEVELOPMENT FOR EXTREME ELECTRICAL METROLOGY

Marija Čundeva-Blajer, Gjorgji Dimitrovski, Viktor Sapundžiovski, Vladimir Dimčev, Kiril Demerdžiev

Faculty of Electrical Engineering and Information Technologies,
"Ss. Cyril and Methodius" University in Skopje,
Rugjer Bošković bb, P.O. Box 574, 1001 Skopje, Republic of North Macedonia
mcundeva@feit.ukim.edu.mk

A b s t r a c t: In the paper analysis findings of the metrological infrastructure for testing and calibration in the area of extreme electrical quantities: very small and very high direct and alternating currents, very small and very high electrical resistances, very high frequencies of electrical signals, as well as electrical inductance and electrical capacitance, are presented. The analysis at the national, regional and international level is conducted within the framework of the scientific research project "Development and Upgrade of Laboratory Resources for Research and Introduction of New Analytical Methods in Electrical Metrology", financed by the Ministry of Education and Science of the Republic of North Macedonia. The needs for measurement, testing and calibration are identified, both for the economy and for enhancement of the laboratory research capacities. The identified gap in the technical readiness (equipment and facilities) of the national laboratories in relation to the international reference laboratories in the field of testing and calibration for extreme electrical quantities is bridged by enhancing the capacities of the Laboratory for Electrical Measurements (LEM) at the Ss. Cyril and Methodius University in Skopje, Faculty of Electrical Engineering and Information Technologies, accredited calibration laboratory in compliance with MKS EN ISO/IEC 17025:2018, with the objective of development and validation of new calibration and test methods, and expansion of the scope of LEM's accreditation in the areas of measurement, testing and calibration in the field of extreme electrical quantities.

Key words: electrical metrology; metrology infrastructure; calibration; extreme electrical quantities

РАЗВОЈ НА ИНФРАСТРУКТУРА ЗА ЕКСТРЕМНА ЕЛЕКТРИЧНА МЕТРОЛОГИЈА

А п с т р а к т: Во трудот се прикажани наодите од анализата на метролошката инфраструктура за тестирање и калибрација во областа на екстремни електрични големини: многу мали и многу високи еднонасочни и наизменични струи, многу мали и многу високи електрични отпорности, многу високи фреквенции на електрични сигнали, како и индуктивност и електрична капацитивност. Анализата е спроведена на национално, регионално и меѓународно ниво во рамките на научноистражувачкиот проект „Развој и надградба на лабораториски ресурси за истражување и воведување нови аналитички методи во електричната метрологија“, финансиран од Министерството за образование и наука на Република Северна Македонија. Воочени се потребите од мерење, тестирање и калибрација, како за стопанството така и за зајакнување на истражувачките лабораториски капацитети. Идентификуваниот јаз во техничката подготвеност (опрема и капацитети) на националните лаборатории во однос на меѓународните референтни лаборатории за тестирање и калибрација на екстремни електрични големини е премостен со подобрување на капацитетите на Лабораторијата за електрични мерења (ЛЕМ) при Универзитетот „Св. Кирил и Методиј“ во Скопје, Факултет за електротехника и информациски технологии, акредитирана за калибрација во согласност со МКС EN ISO/IEC 17025:2018, со цел развој и валидација на нови методи за калибрација и тестирање, како и проширување на опсегот на акредитацијата на ЛЕМ за мерење, тестирање и калибрација во областа на екстремни електрични големини.

Клучни зборови: електрична метрологија; метролошка инфраструктура; калибрации; екстремни електрични големини

1. INTRODUCTION

The metrological and laboratory infrastructure in the Republic of North Macedonia (RNM) is underdeveloped and represents an obstacle in the realization of scientific and R&D projects, which is also a condition for the development of the country's trade and economy [1]. One third of EU legislation relates to measurements and tests, e.g. for the safety of people, the environment, energy, etc., RNM has harmonized to a great extent the legislation in the regulated areas related to these fields, whereby several laws and by-laws were adopted. The existence of appropriately equipped scientific laboratories is fundamental for the quality of the results of measurements and tests, and for ensuring high-level scientific development of the research staff. The metrology of electrical quantities, as an area embedded in all industrial activities, represents a condition for more intensive involvement of Macedonia in industrial and technical cooperation, both at the regional and European level [2]. At the Faculty of Electrical Engineering and Information Technologies (FEEIT), at the Ss. Cyril and Methodius University in Skopje (UKIM), since its foundation, the metrology of electrical quantities has been nurtured. The Laboratory for Electrical Measurements (LEM), an identified independent unit of FEEIT, with implemented quality assurance system, was accredited on 22. 11. 2015 by the Institute of Accreditation of RN Macedonia (IARNM), and on 22. 11. 2019 it was re-accredited in compliance with the international standard MKS EN ISO/IEC 17025:2018, [3, 5], as a calibration laboratory of instruments for electrical quantities, electrical power and energy, with a Certificate for accreditation no. LC-012. The scope of LEM's accreditation covers calibration of instruments and generators for DC and AC voltages and currents, resistance, capacitance, frequency, phase angle, electrical power and energy. LEM is the primary and unique national calibration laboratory for electrical power and energy reference standards, thereby ensuring measurement traceability and uniformity of measurements in this very important area of scientific and legal metrology. The complete measurement and calibration capabilities of LEM are provided in the Annex to the Accreditation Certificate no. LC-012, (iarm.gov.mk) [16]. Since November 2015, the number of calibrations, as well as the type of instruments calibrated in LEM is constantly increasing (more than 400 calibration activities in 2021). LEM is closely related to scientific research conducted at the Institute for Electrical Measurements and Materials (IEMEM) at UKIM-FEEIT, in the field of metrology of electrical quantities. Hence, since 2015, new analytical methods for the calibration of electrical quantities instruments have been continuously introduced in LEM, which have been confirmed and validated on several occasions, through formal expansion of LEM accreditation scope by IARNM with improved the measurement and calibration capabilities (CMC). Calibration activities are carried out in LEM, for the local industry, international corporations operating in technological development zones, conformity assessment bodies (calibration and testing laboratories, inspection and certification bodies), but also for companies and laboratories from the region. One of the most significant activities of LEM is the successful participation in several international inter-laboratory comparisons and proficiency testing schemes, with which LEM successfully proves its top competence and quality in conducting calibrations of electrical quantities, through reports published in the KDBC key comparison database of the International Bureau of Weights and Measures (BIPM) in Paris, and relevant scientific publications [3, 4].

The ensuring of the development and introduction of new laboratory methods, as well as the maintenance of already introduced methods, requires continuous investment in laboratory resources, which is the main goal of the scientific research project financed by the Ministry of Education and Science of the RNM (MES) through the procurement of laboratory resources/reference standards for significant expansion of the LEM accreditation and CMC scope according to МКС EN ISO/IEC 17025: 2018, and for introduction of new calibration methods for instruments, for high direct and alternating currents, high frequencies of electrical signals, very high electrical resistances, very small electrical resistances and electrical inductance. The necessity of these laboratory resources have been identified through the most up-to-date scientific knowledge in electrical metrology, but also following the needs of the industry and other national and regional subjects for calibration services at higher metrology level. The metrology of electrical quantities is a very complex area, in which new scientific breakthroughs are constantly occurring, primarily in two directions:

- expansion of measurement capabilities – development of measurement procedures for new physical quantities, or for extreme values (very high or very small) of physical quantities outside the available measurement ranges, or

- improvement of the existing measurement capabilities – reduction of the measurement uncertainty budget through identification of new influential factors and their correction.

The contribution of the research includes the deepening and expansion of scientific knowledge through:

1. R&D and introduction of a new measurement laboratory procedure for the calibration of a quantity for which there are no traceable national measurement and calibration possibilities – electrical inductance,

2. research and introduction of new measurement laboratory procedures for calibration of very high direct and alternating currents (over 10 A DC and over 120 A AC), for very small resistances (under 100 mΩ), for very high resistances (over 100 MΩ), for high frequencies (above 1 MHz), and

3. reduction of the measurement uncertainties of the already introduced and accredited calibration methods, as well as achieving the lowest uncertainties through in-depth scientific evaluation of the contributions to the budgets of the measurement uncertainties in the newly introduced laboratory procedures, by applying complex mathematical, statistical and numerical methods.

2. ANALYSIS OF THE CURRENT-STATE-OF-THE-ART OF THE BEST MEASUREMENT AND CALIBRATION CAPABILITIES FOR EXTREME VALUES OF ELECTRICAL QUANTITIES

The state-of-the-art analysis of the best measurement and calibration capabilities for unrepresented (electrical inductance) or extreme electrical quantities (high frequencies, very small and very high values of electrical resistance, and very small and very high electrical currents) at the international level started from a survey of published measurement and calibration capabilities of the top national metrology institutes (NMIs) at international level (CMCs in KDBC base of BIPM) [6], but also at the regional level through published CMCs (Calibration and Measurement Capabilities) on the websites of national accreditation bodies for calibration laboratories. Bellow are some of the results of this extensive survey. The extended uncertainty is given with a coverage factor of $k = 2$, with a statistical probability of 95%.

2.1. *Comparison of the best measurement and calibration capabilities at the international and regional level for alternating voltage at high frequencies*

In Figures 1–3, the comparison of the values of the expanded measurement uncertainties of the national metrology institutes (NMIs) at the international and regional level when measuring alternating voltages up to 1 kV at very high frequencies of 500 kHz and 1 MHz, is given.

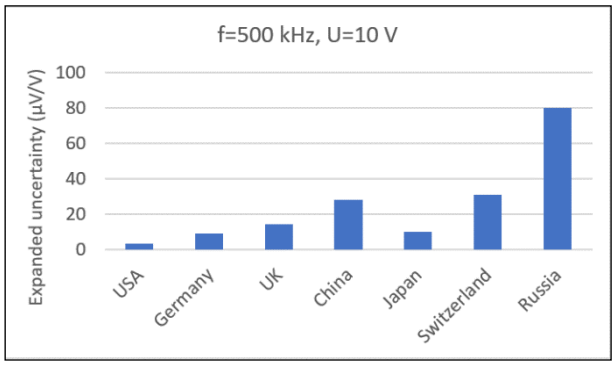


Fig. 1. Expanded measurement uncertainty at 10 V AC voltage at frequency of 500 kHz at the international NMIs level

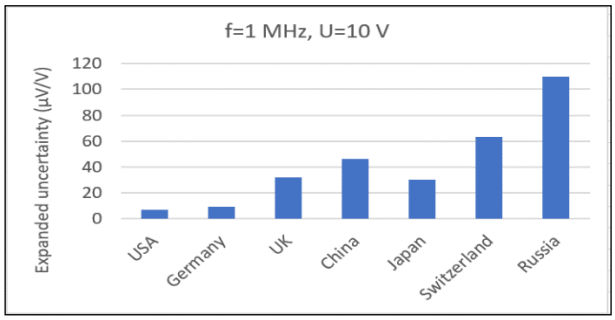


Fig. 2. Expanded measurement uncertainty at 10 V AC voltage at frequency of 1 MHz at the international NMIs level

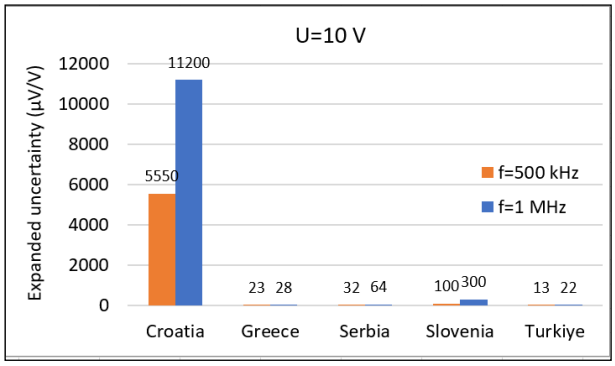


Fig. 3. Expanded measurement uncertainty at 10 V AC voltage at frequencies of 500 kHz and 1 MHz at the regional NMIs level

2.2. *Comparison of the best measurement and calibration capabilities at the international and regional level for high alternating currents*

In Figures 4 and 5, the comparison of the expanded measurement uncertainties of the national metrology institutes at the international and regional level for high alternating currents at high frequencies of 1 kHz and 10 kHz are given.

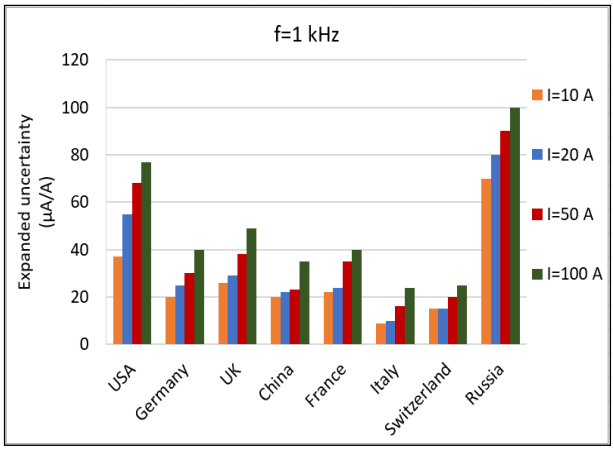


Fig. 4. Comparison of expanded measurement uncertainty of alternating current at frequency of 1 kHz at international NMIs level

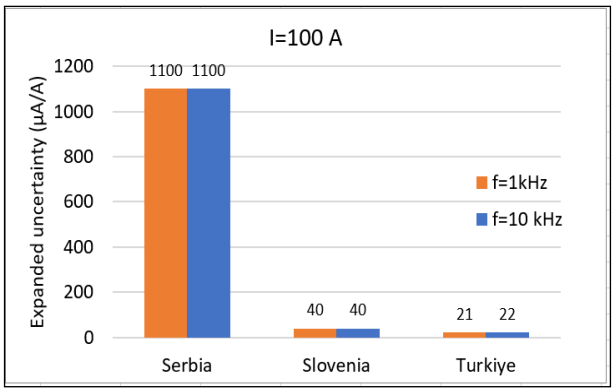


Fig. 5. Expanded measurement uncertainty at 100 A alternating current at 1 kHz and 10 kHz frequencies at the regional NMIs level

2.3. *Comparison of the best measurement and calibration capabilities at the international and regional level for electrical capacitance*

In Figures 6 and 7, the comparison of the expanded measurement uncertainties of the national metrology institutes at the international and regional level for electrical capacitance of 1 μF at high frequencies of 1 kHz are shown.

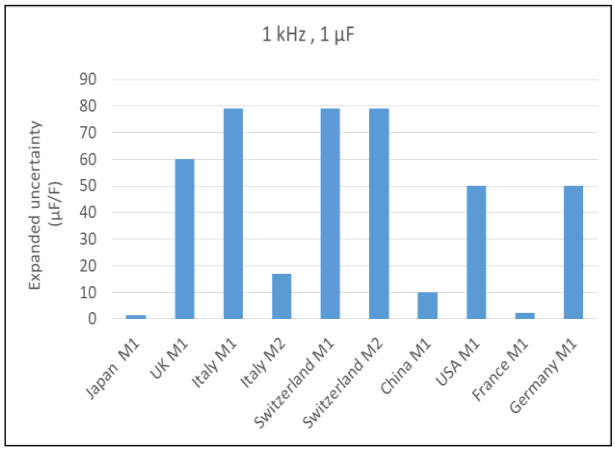


Fig. 6. Expanded measurement uncertainties of electrical capacitance of 1 μF at 1 kHz at the international NMIs level

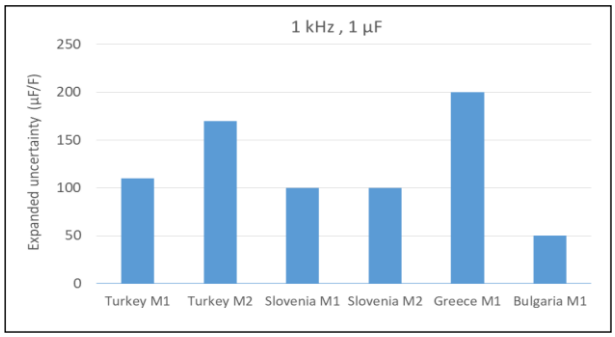


Fig. 7. Expanded measurement uncertainties of electrical capacitance of 1 μF at 1 kHz at the regional NMIs level

2.4. *Comparison of the best measurement and calibration capabilities at the international and regional level for electrical inductance*

In Figures 8 and 9, the comparison of the expanded measurement uncertainties of the national metrological institutes at the international and regional level when measuring electrical inductance of 10 mH at frequency of 1 kHz are displayed.

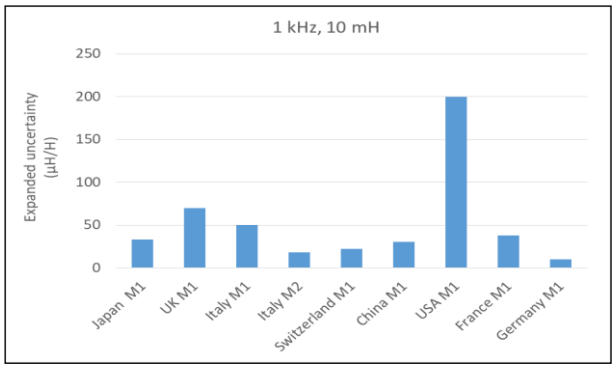


Fig. 8. Expanded measurement uncertainties of electrical inductance of 10 mH at 1 kHz at the international NMIs level

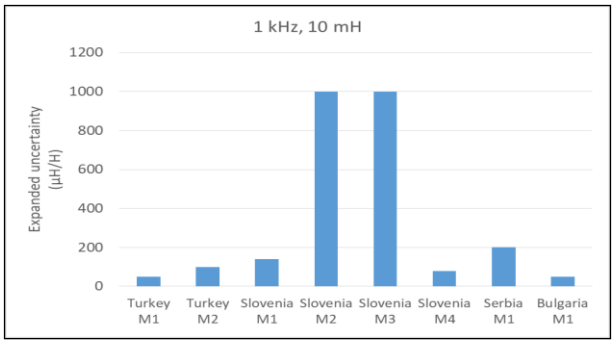


Fig. 9. Expanded measurement uncertainties of electrical inductance of 10 mH at 1 kHz at the regional NMIs level

2.5. *Comparison of the best measurement and calibration capabilities at the international and regional level for low electrical resistance*

In Figures 10 and 11, the comparison of the expanded measurement uncertainties of the national metrology institutes at the international and regional level when measuring a small electrical resistance of 1 mΩ are presented.

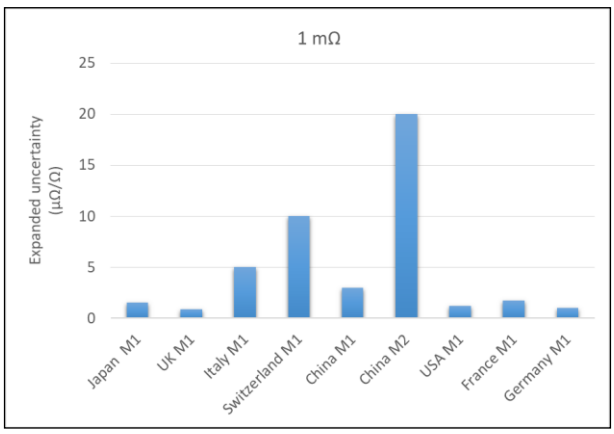


Fig. 10. Expanded measurement uncertainties of electrical resistance of 1 mΩ at the international NMIs level

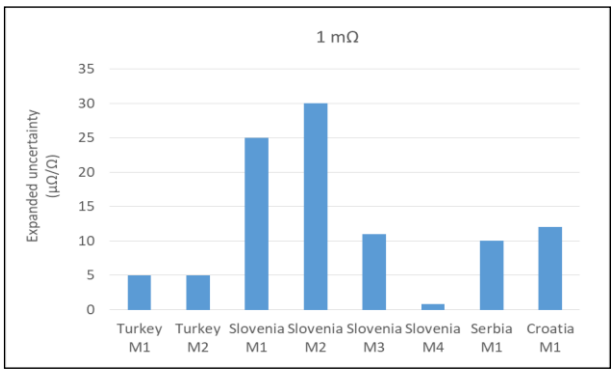


Fig. 11. Expanded measurement uncertainties of electrical resistance of 1 mΩ at the regional NMIs level

2.6. *Comparison of the best measurement and calibration capabilities at the international and regional level for high electrical resistance*

In Figures 12 and 13, the comparison of the expanded measurement uncertainties of the national metrology institutes at the international and regional level when measuring high electrical resistance of 1 GΩ are shown.

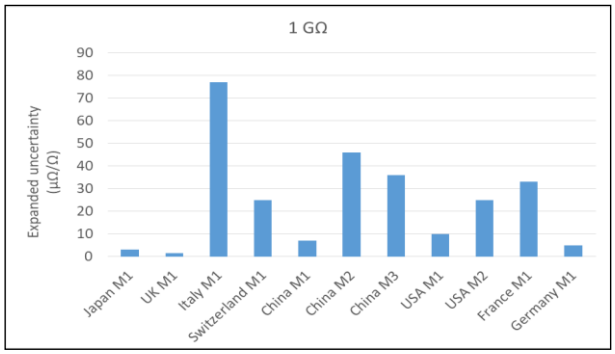


Fig. 12. Expanded measurement uncertainties of electrical resistance of 1 GΩ at the international NMIs level

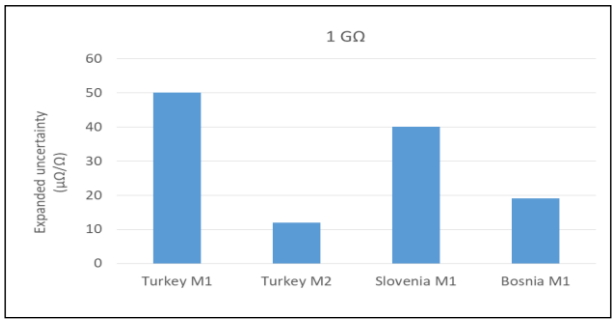


Fig. 13. Expanded measurement uncertainties of electrical resistance of 1 GΩ at the regional NMIs level

2.7. *Measurement and calibration capabilities of the Laboratory for Electrical Measurements at UKIM-FEIT*

In the RN Macedonia, the Laboratory for Electrical Measurements (LEM) at the Ss. Cyril and Methodius University in Skopje, Faculty of Electrical Engineering and Information Technologies, provides the current best measurement and calibration capabilities in the field of electrical quantities, published with the Annex to the accreditation certificate no. LC-012 issued by the IARNM on 26.12.2019.

The technical specifications of the primary and secondary LEM reference standards in Figure 14, as declared by the equipment manufacturers, are given in Table 1, while the published best measurement

and calibration capabilities of the LEM are summarized in Table 2.

Fig. 14. The LEM primary and secondary reference standards for electrical quantities, Agilent 3458A and FLUKE 5500A

T a b l e 1

LEM reference standards uncertainties declared by the equipment manufacturers

Equipment	Measurement range	Uncertainty
DC voltage reference standard FLUKE 732A	10 V 1.018 V 1 V	±0.5 μV/V ±1.5 μV/V ±1.5 μV/V
8½ digit multimeter Agilent 3458A	DC voltage 0 mV up to 1000 V AC voltage 1 mV up to 1000 V, 1 Hz to 50 MHz, sinus DC current 100 nA up to ±1A, AC current 100 μA up to 1 A, 10 Hz up to 10 kHz, sinus Resistance 100 mΩ up to 1 GΩ, Phase angle 0 up to ± 179.99°, Frequency 1 Hz до 10 MHz,	±8 μV/V ±100 μV/V ±14 μA/A ±100 μA/A ±2.2 μΩ/Ω ±0.1 % ±0.1 %
Multifunctional calibrator FLUKE 5500 A	DC voltage 0 mV up to 1020 V AC voltage 1 mV up to 1020 V, 10 Hz up to 500 kHz, sinus DC current 0 up to ±11 A AC current 29 mA up to 11 A, 10 Hz up to 10 kHz, sinus Resistance 0 up to 329.999 MΩ Capacitance 0.33 nF up to 1.1 mF Phase angle 0 up to ± 179.99°, Frequency 0.01 Hz up to 2.0 MHz,	±50 μV/V ±30 μV/V ±10 μA/A ±60 μA/A ±9 μΩ/Ω ±25 μF/F ±0.15° ±25 μHz/Hz

T a b l e 2

Published LEM best measurement and calibration capabilities

Physical Quantity	Range	Uncertainty
DC voltage	10 mV “to 1020 V	22 μV/V
AC voltage	10 mV to 1020 V, 10 Hz to 1 MHz, sinus	35 μV/V
DC current	0 to ±11A	80 μA/A
AC current	50 μA to 11 A	170 μA/A
Resistance	0.1 Ω to 100 MΩ	20 μΩ/Ω
Capacitance	0.33 nF to 1.1 mF	25 μF/F
Active power Reactive power Apparent power	Up to 67.2 kW Up to 67.2 kVAr Up to 67.2 kVA	0.017 %
Electrical energy		0.018 %

3. BRIDGING THE METROLOGICAL GAP IN THE AREA OF EXTREME ELECTRICAL QUANTITIES BY ENHANCING THE CAPACITIES OF LEM

As a result of the perceived gap in measurement and calibration possibilities between top international laboratories, and taking into account the regional state of the metrological infrastructure in the area of electrical quantities, an analysis of the international supply of reference standards for electrical quantities that are not covered by the existing LEM reference standards has been carried out.

Based on the conducted analysis, LEM has defined a detailed technical specification for the procurement of reference standards, for significant expansion of the measurement and calibration capabilities of LEM.

Table 3 shows the detailed technical specifications of reference standards, acquired within the frame of the scientific research project "Development and Upgrade of Laboratory Resources for Research and Introduction of New Analytical Methods in Electrical Metrology", which is implemented within the program for financing scientific research projects of special and public interest for 2021 (support for the development of laboratory resources) by the Ministry of Education and Science of the Republic of North Macedonia.

Table 3

Detailed technical specifications of reference standards, acquired within the scientific project "Development and Upgrade of Laboratory Resources for Research and Introduction of New Analytical Methods in Electrical Metrology" for expansion of LEM's CMC for extreme electrical quanitites

Multifunctional calibrator Transmille 4015	
Technical specifications	
Measurement range	Best annual accuracy:
– DC voltage 0 – ±1025 V	±15 ppm
– DC current 0 – 30 A	±50 ppm
– AC voltage 20 mV – 1000 V, 10 Hz – 500 kHz	0.015%
– AC current 20 µA – 30 A, 10 Hz – 30 kHz	0.04%
– Electrical resistance (passive) 0 – 1 GΩ	40 ppm
– Electrical capacitance (passive) 1 nF – 10 µF	0.25%
– Frequency 1 Hz – 10 MHz	30 ppm
– Temperature (for thermocouples calibration) J / K / T / R / S / B / U / N / E / L / U / C / 10 µV°C	±0.09 °C
– Electrical resistance (simulated) 0 – 1 GΩ	100 ppm

Supplement to the multifunctional calibrator for calibration of oscilloscopes with frequency range up to 600 MHz Transmille sPC600	
Technical specifications	
Range	Resolution
2 mV/Div to 10 mV/Div	10 nV
20 mV/Div to 100 mV/Div	100 nV
200 mV/Div to 2 V/Div	1 µV
5 V/Div to 20 V/Div	10 µV
50 V/Div	100 µV
Range	Best annual accurac
DC voltage (2 mV to 50 V/Div)	0.01 %
AC volatge (2 mV to 50 V/Div)	0.1 %
Time base (2 ns/Div. to 5 s/Div.)	5 ppm
Frequency (reference frequency 50 kHz)	30 ppm
Rise time/fall	1 ns
Wave forms	Combined at least up to 100 ns

Supplement to the multifunctional calibrator for calibration of instruments for inductance (coils) with specifications for 1 kHz and accuracy of ± 50 µH Transmille IND			
Technical Specifications			
Electrical Inductance	Q-factor	Display resolution	Best annual accuracy
1 mH	1	100 nH	0.5 %
10 mH	2.8	1 µH	0.5 %
19 mH	3.8	1 µH	0.5 %
29 mH	4.7	1 µH	0.5 %
50 mH	6.1	1 µH	0.5 %
100 mH	8.6	10 µH	0.5 %
1 H	29	100 µH	0.5 %
10 H	110	1 mH	0.5 %

Supplement to the multifunctional calibrator for calibration of instruments for picoamp currents and adapter for high teraohm resistance Transmille EA008			
Technical specifications			
Measurement range	Resolution	Best annual accuracy in % of reading	Best annual accuracy in % of range
10 nA	1 pA	0.5	0.4
100 nA	10 pA	0.5	0.4
1 µA	100 pA	0.5	0.4
10 µA	1 nA	0.5	0.4
100 µA	10 nA	0.5	0.4

Supplement (high current coil) to the multifunctional calibrator for calibration of instruments for currents up to 1500 A (for frequencies from 0 to 60 Hz) Transmille EA002	
Technical specifications	
Measurement range	Best annual accuracy
Input 0 of 30 A Frequency from DC – 30 Hz to 60 Hz Effective output 0 to 60 A	0.35% + 0.008 A
Input 0 to 30 A Frequency from DC – 30 Hz to 60 Hz Effective output 0 to 300 A	0.41% + 0.01 A
Input 0 to 30 A Frequency from DC – 30 Hz to 60 Hz Effective output 0 to 1500A	0.24% + 0.04 A

Reference standard resistance decade from 1 mΩ to 1 Ω with resolution of 1 mΩ IET Labs 1433-01			
Technical specifications			
Resolution of change	Total resistance	Best stability (±ppm/year)	Accuracy
1 mΩ	10 mΩ	50	±0.01%
10 mΩ	100 mΩ	50	±0.01%
100 mΩ	1 Ω	50	±0.01%

Reference standard resistance decade from 10 Ω to 1 TΩ for voltage of 5 kV IET Labs HRRSQ	
Technical specifications	
Characteristics	Value
Electrical resistance	from 10 Ω до 1 TΩ
Accuracy class	0.01%
Voltage level	5 kV
Temperature coefficient	5 ppm/°C
Voltage coefficient	0.2 ppm/V

All the acquired equipment is with calibration certificates insuring measurement traceability to SI units, from qualified and competent calibration laboratories (accredited by an accreditation body that is on the list of signatories of the MLA for the area of calibration EA-Mutual Recognition Agreement, or the Agreement on mutual recognition within the framework of ILAC-International Laboratory Accreditation Cooperation, or a national metrology institute signatory to the CIPM MRA- Agreement on mutual recognition of national standards and calibration and measurement certificates issued by national metrology institutes), which is in accordance with the Regulations for ensuring measurement traceability of RNM, published by IARNM.

4. DEVELOPMENT OF NEW CALIBRATION PROCEDURES AND MODIFICATION OF EXISTING PROCEDURES IN LEM FOR CALIBRATION OF INSTRUMENTS FOR EXTREME ELECTRICAL QUANTITIES WITH EXTENDED CMC

After the acquisition of the reference standards, a scientific approach will be taken to put the acquired equipment into research function, through the development of completely new laboratory procedures (calibration of inductance meters, calibration of high-frequency meters-oscilloscopes and function generators), as well as modification of the existing laboratory procedures for extreme values of electrical quantities and/or calibration of new types of meters (calibration of meters for high direct and alternating currents, calibration of meters for very small resistances-microohmmeters, calibration of meters for very high resistances – giga and teraohmeters).

The principles of best laboratory practice will be deployed in accordance with internationally standardized guidelines (BIPM, Euramet, ILAC, NIST, IEEE, IEC and EN guidelines/standards). In each of the measurement procedures, the measurement traceability chain continuity to national or internationally recognized primary standards will be ensured and scientific analysis of the influencing factors in the budget of measurement uncertainty will be conducted by applying advanced mathematical and statistical metrological methods, including non-conventional techniques from probability and statistics (Monte Carlo or Bayesian statistics), but also some numerical (method of least squares, finite element method) and stochastic methods.

Quality assurance and confidence in the results of newly introduced or modified calibration procedures will be achieved through internal and external quality measures (determining the degree of repeatability and reproducibility of the method, inter-laboratory comparisons and participation in proficiency testing schemes).

CONCLUSIONS

To achieve long-term sustainability of the laboratory facilities, after the full introduction of the new and modified laboratory procedures, their accreditation is planned, with the objective of expanding the measurement and calibration capabilities of LEM. The granting of an expanded scope of accreditation to LEM and its official publication on the IARNM website will enable further wider promotion and exploitation of the project results, i.e. provision of new calibration services for the research infrastructure and the industry in the country, but also widely in the region.

During the implementation of the project, young scientific personnel are directly trained and introduced to the new laboratory procedures, and the entire acquired equipment will be made available free of charge for research and education purposes.

REFERENCES

[1] Čundeva-Blajer, M., Dimčev, V,, Demerdžiev, K. et. al., *Development and Upgrade of Laboratory Resources for Research and Introduction of Novel Analitical Methods in Electrical Metrology*, Scientific project financed by the Ministry of Education and Science of RN Macedonia, Skopje, 2021–2023 (on-going).

[2] Arsov, L., Čundeva-Blajer, M. (2013): Establishing a metrological infrastructure and traceability of electrical power and energy in the R. Macedonia, *ACTA IMEKO*, December 2013, Vol. **2,** No. 2, pp. 86–90, www.imeko.org

[3] Demerdžiev, K., Čundeva-Blajer, M., Dimčev, V., Srbinovska, M., Kokolanski, Z. (2018): Improvement of the FEIT laboratory of electrical measurements best CMC through internationally traceable calibrations and inter-laboratory comparisons, *Conf. Proc. of Int. Conf. ETAI 2018, Struga, R. Macedonia, 20–22 September 2018* (ETAI 6-4).

[4] Velychko, O., Karpenko, S., Kazakova, E., Gubler, G., Gelovani, M., Abasbekova, E., Cayci, H., Sluciak, J., Čundeva-Blajer, M., Lei, W., Ariuntungalag, J., Bartolomew, J., Alorobaish, A. M., Halawa, M. (2019): Final Report on COOMET key comparison of power (COOMET.EM-K5), *Metrologia,* Vol. 56, No. 1A, 2019, pp. 01010, (https://iopscience.iop.org/article/10.1088/0026-1394/56/1A/01010)

[5] МКС EN ISO/IEC 17025 "General requirements for the competence of testing and calibration laboratories", *Cenelec*, Brussels, 2018.

[6] www.bipm.org (retrieved on: 03.06.2022).

[7] RU 7.2.01 *Working Instruction on Calibration of Multimeters*, LEM-FEIT, 2019.

[8] RU 7.2.02 *Working Instruction on Calibration of Electricity Reference Standards and Meters*, LEM-FEIT, 2019.

[9] RU 7.2.03 *Working Instruction on Calibration of Multifunctional Calibrators*, LEM-FEIT, 2019.

[10] RU 7.6.01 *Working Instruction on Expression of Measurement Uncertainty – General Procedure*, LEM-FEIT, 2019.

[11] EURAMET cg-15, *Guidelines on the Calibration of Digital Multimeters*, Ver. 3 02/2015.

[12] EURAMET cg-7, *Guidelines of Measuring Devices for Electrical Quantities, Calibration of Oscilloscopes*, Ver. 1.0, 06/2011.

[13] Čundeva-Blajer, M., Dimčev, V., Srbinovska, M., Kokolanski, Ž. (2016): A Contribution to the metrology infrastructure through accredited and traceable electrical measurements and calibrations, *Conf. Proc. of Int. Conf. ETAI, Skopje, R. Macedonia.*

[14] *Evaluation of Measurement Data — Guide to the Expression of Uncertainty in Measurement* (GUM), JCGM 100 with member organizations (BIPM, IEC, IFCC, ILAC, ISO, IUPAC, IUPAP and OIML), 2008.

[15] ISO/IEC 17043:2010 *Conformity Assessment – General Requirements for Poficiency Testing*, Geneve 2010

[16] www.iarm.gov.mk (retrieved on: 4.12.2022).

Journal of Electrical Engineering and Information Technologies, Vol. **7,** No. 2, pp. 111–114 (2022
In print: ISSN 2545–4250
On line: ISSN 2545–4269

INSTRUCTIONS FOR AUTHORS

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

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

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

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

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

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

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

SUBMISSION

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

JEEIT@feit.ukim.edu.mk.

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

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

PREPARATION OF MANUSCRIPT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

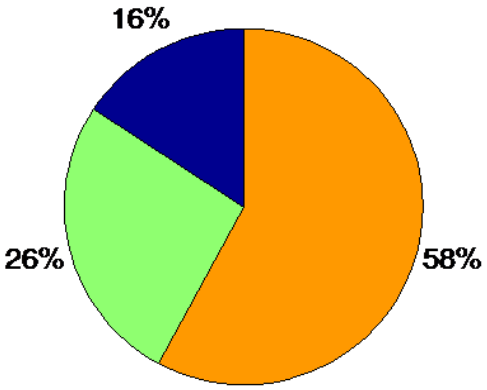


Fig. 1. Example of a graph and a single-line caption

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

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

– the colours used in each figure contrast well,

– the image used in each figure is clear,

– all text labels in each figure are legible.

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

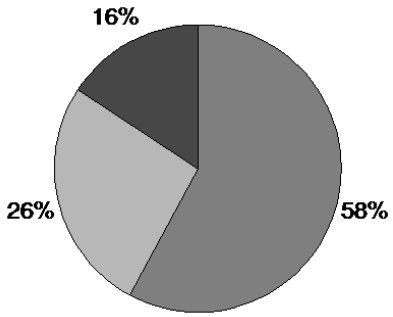


Fig. 2. Example of a graph and a single-line caption

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

Footnotes are also not permitted.

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

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

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

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

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

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

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

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

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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