ORIGINAL ARTICLE

A High-Performance, Secure Custom Electronics Circuit for Biopotential Measurement and Processing

Arrigo Palumbo [1], Barbara Calabrese [1*], Nicola Ielpo [1], Remo Garropoli [2], Patrizia Vizza [1], Andrea Demeco [3], Vera Gramigna [1]

[1] *Department of Medical and Surgical Sciences, University Magna Graecia, Viale Europa 88100 Catanzaro, Italy*

[2] *Garropoli Computer Science Consulting, 87100 Cosenza, Italy*

[3] *Corchiola Computer Science Consulting, 87100 Cosenza, Italy*

*Corresponding Author: Barbara Calabrese
Email: calabreseb@unicz.it

Received: 28 December 2022 / Accepted: 06 March 2023

Abstract

Purpose: In this paper, we propose a secure wearable and portable device aiming to (i) monitor physical activity in medical and clinical rehabilitation, (ii) evaluate the subject's movements in sports environments, and (iii) monitor wellness indicators.

Materials and Methods: The innovative low-power custom circuit can acquire, pre-process, digitalize, and transmit EMG signals to a Raspberry PI4 device via a low-energy Bluetooth module. The Raspberry PI4 is a hub that sends data to a cloud-based system for remote monitoring and processing. The best cybersecurity practices have been implemented: firewall, anti-DDoS and SELinux.

Results: We have assessed the system's vulnerability before and after the system's hardening. SELinux makes the system safer and prevents unauthorized access to patients' data health by tampering with the devices.

Conclusion: Adopting IoT systems in telemedicine requires greater attention to cybersecurity. It is necessary to implement security mechanisms to guarantee the privacy of patient's health data.

Keywords: Telemonitoring; Telerehabilitation; Bio-Signal Acquisition; Internet of Things; Cybersecurity; Electromyography.

DOI: https://doi.org/10.18502/fbt.v11i3.15881

Frontiers in BIOMEDICAL TECHNOLOGIES

1. Introduction

Monitoring and analysis of bioelectrical signals (i.e., the Electrocardiogram (ECG), Electromyogram (EMG), and Electroencephalogram (EEG)) are essential to support the diagnosis, prevention, and examination of a range of clinical situations. Wearable devices allow the remote and outpatient monitoring of physiological parameters and signals [1-6]. Therefore, patient monitoring through mobile health (m-health) applications becomes increasingly challenging for the scientific community and large Internet of Things (IoT) companies.

The use of wearable devices for detecting biomedical signals is rapidly expanding in the medical field to monitor and evaluate clinical parameters and in other areas, for example, sports monitoring or rehabilitation [7] or well-being. This development is strongly linked to the evolution of acquisition techniques, integrated circuits that are becoming cheaper, and technological connectivity. In the literature, there are many contributions proposed in this direction. Nascimento *et al.* [8] present a review of sensors and systems for rehabilitation and health monitoring, focusing on analyzing the implementation of sensors for biomedical applications. In particular, the mentioned study divides the sensors into three macro groups:

- Sensors for health care, home medical assistance, and real-time monitoring of the state of health. Also included in this category are wearable devices, such as systems for monitoring patients at home or athletes while performing physical exercises;
- Sensors and physical rehabilitation systems aimed at health care and rehabilitation;
- Assistance systems in the communication phase between patient and doctor are intended to support the physical movement of people with mobility or communication problems.

Zhao *et al.* [9] present a wearable device for upper limb monitoring aimed at rehabilitation. It integrates ECG and EMG sensors. The ECG / EMG signals are suitably filtered, amplified, digitized, and transmitted via a low-energy Bluetooth module to a remote receiver (such as a smartphone or laptop). A software platform was also developed for data analysis and the display of ECG / EMG information integrated into the control module of the robotic glove. The results provided a new technique for monitoring the individual information extracted from ECG and EMG and a valuable technical reference to improve the rehabilitation of the upper limbs based on specific treatment conditions and user requests. Wu *et al.* [10] propose the development of a low-cost EMG sensor network consisting of four surface EMG sensors and PC software. The designed EMG sensor consists of electrodes, a signal conditioning circuit, an A / D conversion module, a microcontroller, a WI-FI communication module, a lithium battery, and a power module. Starting with raw EMG signals, the system extracts a set of time-domain functionalities to train a neural network in MATLAB to recognize specific movements. Uktveris *et al.* [11] present the design and evaluation of a compact, modular, battery-powered EEG signal acquisition board based on an integrated ADS1298 analog front-end chip. This type of card's introduction solves the EEG scalability problem by effectively reconfiguring the hardware for specific applications, allowing the acquisition of up to 64 EEG channels at sampling rates from 250 Hz to 1000 Hz. The acquired data is then transferred via Bluetooth or WI-FI interface.

The study conducted by Mangal [12] focuses on wireless sensor technology to develop a service platform using smart wear for patient monitoring. In particular, the proposed research considers the acquisition of a 3-lead ECG to detect the severity of cardiovascular disease. The ECG signal will also be accompanied by the addition of the EMG signal to determine the cardiac signal and see muscle contraction. The results of this study will be helpful in the realization and control of the robotic hand using EMG electrodes to detect muscle contraction and relaxation of the human hand. Al-Khawaja *et al.* [13] contribute to remotely monitoring an individual's health status to identify abnormal conditions and intervene early. Therefore, the authors develop an intelligent health monitoring system capable of observing older people remotely by tracking physiological data to detect specific disorders and support early intervention. The system consists of wearable wireless sensors, computer hardware, networks, and software applications interconnected to exchange data and provide services in an assisted environment. Sensors and actuators are connected to

patient gateways for sending medical data to a data center, which becomes available for monitoring. Jani *et al.* [14] present an ECG / EMG sensor with low power consumption and cost. The sensor consists of a single discrete component board. It acquires ECG / EMG signals non-invasively and sends them to the ADC of a microcontroller for post-processing and analysis. This type of sensor can be used in various applications, including controlling and monitoring muscle movements and prosthetic instruments. Nguyen *et al.* [15] are involved in studying, applying, and integrating the ADS1299 integrated circuit to construct a portable EEG system used in specific EEG signal analysis or Brain-Computer Interface applications. The resulting system is an EEG front-end with STM32F4-controlled ADS1299 and an integrated real-time interface suited for brain activities. Therefore, the objective of the proposed work is to use the ADS1299 for the acquisition of EEG signals in an effective way aimed at the realization of an EEG front-end system for the collection of high-frequency data, but wearable, of compact size, wireless, low cost and with real-time acquisitions.

The IoT market has grown significantly, with many IoT products available to consumers, businesses, and industries. It is estimated that IoT will increase to a trillion devices by 2035. At the same time, it is well known that there are some security risks related to IoT devices. The IoT ecosystem includes the following components: (i) Cloud, which pro-vides data storage and global computing services; (ii) gateway, which interfiles the end-point with the cloud component and (iii) edge, the end-point device that contains sensors and actuators. Each level requires its security considerations and faces several threats and attacks. Meeting the different security requirements of versatile IoT use cases is also a big challenge, particularly since third-party hardware and software components used on devices need to consider the security requirements of the final device. Integrating safe design practices within the IoT product lifecycle is critical to protecting against threats such as counterfeiting, privacy attacks, system compromise, and damage, which can cause severe reputational damage [4-6].

This paper proposes a novel, high-performance, secure custom electronics circuit for biopotential remote measurement and processing. The module acquires, preprocesses, digitalizes, and transmits EMG signals via a low-energy Bluetooth module to a Raspberry PI4 device. The Raspberry PI4 is a hub that sends data to a cloud-based system for remote monitoring and processing. Specifically, in addition to the security of the cloud, we have also paid attention to the security aspects related to the gateway, as our system allows the technician/medical staff to set and adjust the acquisition parameters, intervening remotely directly on the monitoring system. Specific security mechanisms have been implemented to safeguard the security of the Raspberry Gateway, which is the system's weak link. Consequently, in addition to avoiding problems related to the confidentiality and integrity of the data acquired by limiting access only to authorized persons, we wanted to prevent any active attacks that could change the device settings.

The paper is organized as follows: section 2 describes the architecture of the acquisition module (edge) and transmission module (gateway). Section 3 presents and discusses some experimental results relative to security tests. Finally, Section 4 concludes the paper.

2. Materials and Methods

The architecture of the proposed system for remote biopotential acquisition and processing is shown in Figure 1. We have designed a custom electronic circuit that interfaces to EMG electrodes for signal acquisition and digital conversion. EMG data are then transferred via Bluetooth to Raspberry PI (Raspberry PI Foundation, https://www.raspberrypi.com) for

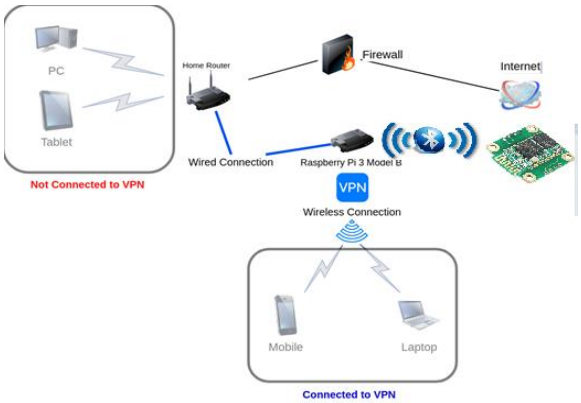

Figure 1. System's overview

further processing and transmission to a cloud-based system for storage and analysis.

Precisely, the proposed custom acquisition circuit solution essentially consists of 4 macro-blocks: (i) signal pre-conditioning with a protection circuit and a first amplification stage; (ii) signal processing with relative low-pass, high-pass, and notch filters and amplification; (iii) data conversion and transmission with front-end circuit, second amplifier stage, Sigma-Delta converter and microcontroller for transmission in Bluetooth; (iv) power supply with relative different circuit components in the case of the battery-powered 4-channel solution (see Figure 2).

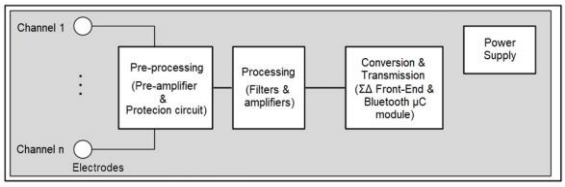

Figure 2. Biopotential acquisition circuit elements

Raspberry PI4 was adopted as part of a telemedicine project [16-18] and used as a gateway for receiving data from Bluetooth sensors to capture bio-signals (such as electromyographic EMG signals) and send them to a system in the cloud through RESTful services. In addition, the Raspberry has been configured as an access point. An app configures the system through Wi-Fi, such as Bluetooth pairing between the acquisition circuit and the Raspberry IoT gateway. The Raspberry connects to the Internet via the Ethernet cable.

A detailed description of the hardware modules is given in the following paragraphs.

2.1. A Custom Biopotential Acquisition Circuit

A custom device for acquiring, conditioning, processing, and transmitting Electromyographic (EMG) signals (see Figure 3) was realized. The proposed solution is a four-channel-based solution powered by rechargeable lithium-ion batteries.

This section describes all the circuit blocks used in the board construction, explaining their characteristics and detailing the design choices to satisfy the required requirements.

2.1.1. Preprocessing

Given the nature of the biopotentials and their minimal amplitude value (of the order of µV or mV), at the input of the acquisition circuit, it is necessary to insert a first amplification stage, called the pre-processing stage. This stage implements an overvoltage protection circuit that has the task of regulating the input voltage of the device to prevent input voltage peaks between the electrodes (indicated as A in Figure 4) and a pre-amplification stage that allows increasing the amplitude level of the input signal to be suitably processed (shown as B in Figure 4).

In this phase, the gain offered by pre-amplification must be low; otherwise, unwanted noise and signal would be amplified erroneously in addition to the proper signal. This is because upstream of the pre-amplifier, there is yet to be any level of filtering, which also causes unwanted signal components to pass through.

The pre-amplification stage was built with the Texas Instruments INA126 instrumentation amplifier [19]. The choice of this component is linked to its high precision and low noise characteristics that make it suitable for biomedical applications, especially for amplifying EMG, ECG, and EEG signals. The gain setting (10 V/V) is adjusted using an ex-ternal resistor, as depicted in Figure 3.

2.1.2. Filtering

The filtering stage within a biomedical signal acquisition and conditioning system must attenuate and eliminate unwanted components that match the signal of interest during acquisition.

Therefore, the analog filtering technique is widely used in biomedical device design because it eliminates unwanted signals (such as physiological artifacts).

The filtering chain is located downstream of the pre-amplification stage and is composed of three blocks of filters (Figure 4):

- high pass filter;
- notch filter;
- low pass filter.

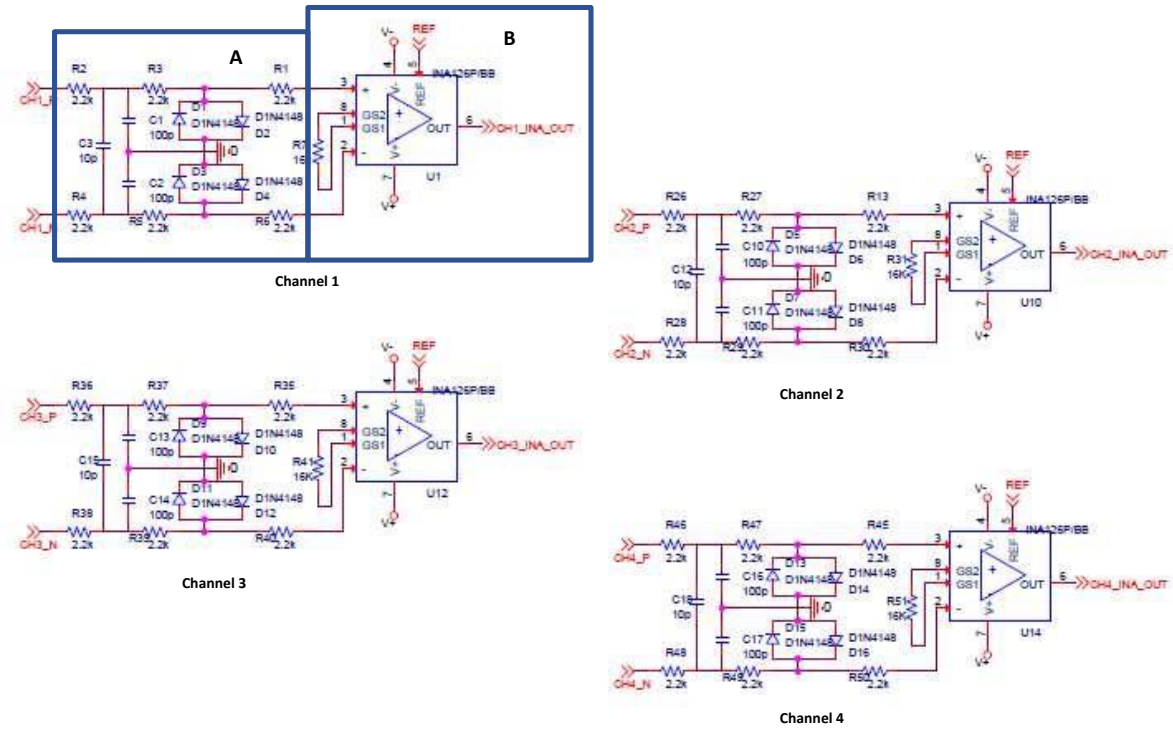

Figure 3. Pre-processing stage of the four-channel acquisition module. Each channel is depicted (Channel 1, Channel 2, Channel 3, and Channel 4 in the overvoltage protection circuit (A), and the pre-amplifier stage (B) is indicated only for Channel 1

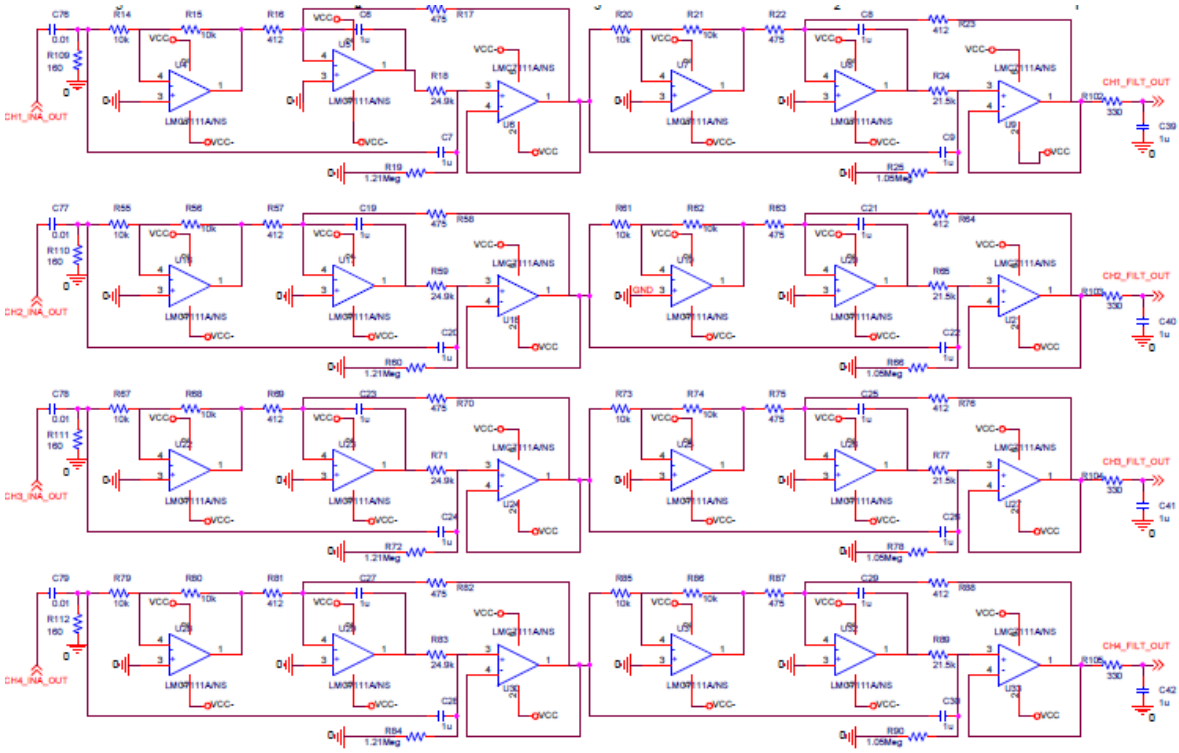

Figure 4. Schematic of the filtering circuits for the four-channels front-end

The high-pass filter and the low-pass filter allow only the frequency band of the signal of interest, consequently attenuating all the other unwanted frequency components outside the band of interest. Specifically, the cut-off frequencies of high-pass and low-pass filters are 0,1 and 500 Hz. The notch filter (50/60 Hz) acts as a bandwidth filter since it allows the elimination of or, in any case, significantly reduces the frequency content at 50 Hz (see Figure 5). The notch filter is of the 4th order of Butterworth type. The attenuation at the frequency of 50 Hz is about -70 dB. Compared to the reference signals, these filters' cut-off frequencies vary and can be easily set by acting directly on the circuitry.

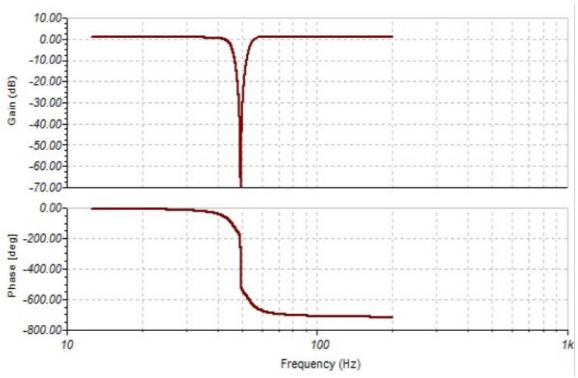

Figure 5. Notch's filter frequency and phase responses

2.1.3. Amplifier and A/D Conversion

Texas Instruments ADS1294 [20] represents the first fully integrated Analog Front End (AFE) for medical device ap-plications, especially for monitoring ECG, EEG, and EMG signals. ADS1294 has an energy efficiency of 1 mW / channel, drastically reducing the number of elements required compared to a discrete component design and significantly lowering consumption (up to 95%) compared to classic implementations. The features integrated into the ADS1294 mainly include several low-noise Sigma-Delta converters flanked by an equal number of programmable gain amplifiers, again with low noise. The internal amplifiers are programmed to a gain of 12, which will be helpful in the design phase to in-crease the entire gain of the circuit board (Figure 6). The typical noise value referred to the input of 4 µVpp is higher than the thresholds provided by the CE / IEC 60601-1 standard, thus ensuring accurate measurements in portable devices and medical equipment with high channel density [20]. The Sigma-Delta converters, present in the circuit and implemented in the ADS1294, convert the analog EMG input signals into discrete data. The Sigma-Delta converters are 24-bit and are present on each acquisition channel with a data rate that can be programmed from 250 SPS to 32 kSPS.

2.1.4. Data Transmission

The last step in the signal acquisition and conditioning chain concerns transmitting the converted data to the gateway device for further processing and transfer to the cloud. The choice of the type of transmission and its consequent circuit implementation respects the design requirements of portable and low-consumption applications. The CC2640 component [21] from Texas Instruments was chosen to implement the part relating to the transmission. This device is a 2.4 GHz wireless microcontroller, supports the Bluetooth® 5.1 Low Energy standard, and is optimized for low-power wireless communication applications in the medical field. It guarantees high performance, low power consumption, and low costs, fully satisfying the required design specifications. Moreover, the Bluetooth module satisfies the transmission link speed. The internal microcontroller is a Powerful Arm® Cortex®-M3 [22].

As for the antenna, as can already be seen from the block diagram figure, CC2640 provides an external 50 Ohm antenna and allows for multiple implementable configurations. For the study, especially given the physical construction of the board and to meet the low cost and small size requirements, it was decided to use a circuit solution that incorporated both the CC2640 and the antenna part together to have a single component, thus reducing the external circuitry supplied with the CC2640 and ensuring correct formulation of the RF part. The element enclosing the CC2640 and RF antenna is the Bluetooth Low Energy RF-BM-4044 module from Shenzhen RF-star Technology Co., Ltd [23]. This solution is relatively recent (its release date to May 2020). In particular, the module that best meets the required characteristics is RF-BM-4044B2 which has a PCB antenna, a CC2640R2FRSM [24] with 32-bit ARM CortexTM-M3 processor and an operating frequency of 48.0 MHz and a size of 11.2 x 16.6 mm.

RF-BM-4044B2 significantly reduces the problems inherent in the antenna design, which would have required a detailed and in-depth study and an ad hoc design.

In addition to the two main components of this conversion and transmission blocks, two connectors have been used, necessary for programming the registers of the microcontrollers of the two chips ADS1294 (amplification and conversion) and RF-BM-4044 (transmission). The component of choice for this type of connector is the 8-position TE Connectivity (TE) Micro-Match (see the components "J2" and "J8" in Figure 6).

2.1.5. Power Supply

The four-channel acquisition circuit board is battery-powered and requires an external rechargeable battery. The battery chosen is lithium-ion with a voltage of 3.7 V. The choice fell on this type of battery because it is the most used for portable applications in the biomedical field. Moreover, lithium-ion batteries are characterized by low weight, small size, and energy consumption, making them very advantageous for their use in portable medical devices.

The battery voltage is suitably stabilized at an output value of 3 V. A voltage regulator has been used to produce two voltage values, +3 V and -3 V, necessary for powering some circuit components (instrumentation amplifiers and operational amplifiers). The two supply voltage values at +3 V and -3 V are identified in the circuit as V+ and V-, respectively. The schematic of this section is reported in Figure 7. The first component of the power chain is represented by BQ24232, which acts as the charging circuit for the 3.7 V Li-ion battery through the micro-USB connector. The output voltage is the input of the second component of the chain, i.e., the TPS61220, which supplies a fixed voltage at 3V in the output so as not to influence the power supply of the entire circuit concerning the charging/ battery discharge. This voltage enters the last component of the chain, LM27762, which regulates the output at two voltage levels, one positive at +3 V and the other negative at -3 V. Added to these components are the connectors for recharging the battery for connecting the electrodes and the battery.

BQ24232 (Texas Instruments) is a USB-friendly lithium-ion charger and power path management IC; it then acts as a lithium-ion battery charger via a micro-USB interface [28].

On the other hand, the voltage stabilizer was implemented using the Texas Instruments TPS61220 component [25]. The voltage stabilizer chosen is nothing more than a boost converter. It performs the function of stabilizing the output voltage at a constant voltage value (3V in this case) so as not to be dependent on the charge-discharge phase of the battery, which, otherwise, would affect the operation of the whole circuit. In this way, even if the battery voltage drops be-low 3.7V, at the output from the stabilizer, the voltage is kept fixed at a constant value—the voltage regulator.

The component chosen for its implementation is LM27762 from Texas Instruments. LM27762 adjusts the input voltage to two output values, one positive and the other negative, necessary for the power supply of all the circuit com-ponents chosen for the

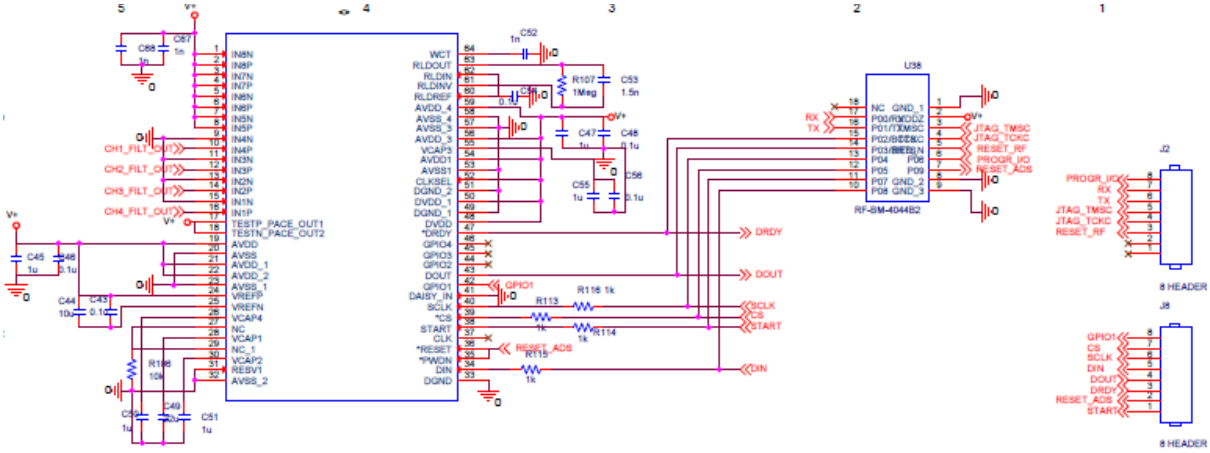

Figure 6. Schematic of amplification, A/D Conversion and Transmission modules

development of the board, including the power supplies of the instrumentation amplifiers and of the operational amplifiers that they require a double power supply (positive and negative). In this specific case, the stabilized output voltage of the TPS61220 is adjusted to the values of + 3V and -3V, respectively.

2.1.6. Circuit Implementation

Given the circuit complexity and the high number of components, a positioning criterion was defined which provides for the use of the two external layers, TOP and BOTTOM, according to a precise rule: all the components relating to the power supply and pre-conditioning have been positioned on the TOP side of the board. In contrast, all the components relating to the filtering block and A/D conversion have been placed on the BOTTOM side, except for the RF_BM_4044 part, which contains the antenna and has been set on the TOP side. The positioning of the components took place following the most common placement rules, including:

- place the components directly connected as close as possible to reduce the interconnection tracks;
- place similar components close together and always in the same direction;
- for op amps connected with other components (such as resistors and capacitors) in forming specific configurations, recreate that configuration also on the PCB by placing the operational in the center concerning the other components;
- position the components concerning a uniform arrangement (all vertically or all horizontally) and aligned concerning a grid;
- position the connectors on the top side of the board.

The result of positioning the components on the board is shown in Figure 8. The component that goes beyond the edge of the board is RF_BM_4044, and the part that protrudes is the antenna.

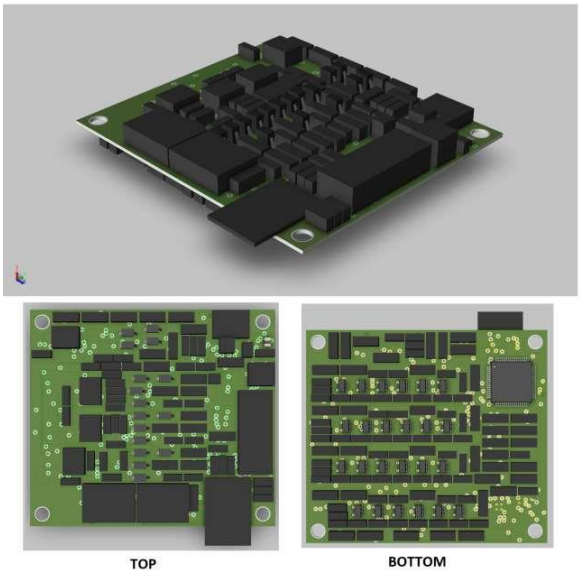

Figure 8. 3-D view of the proposed acquisition system

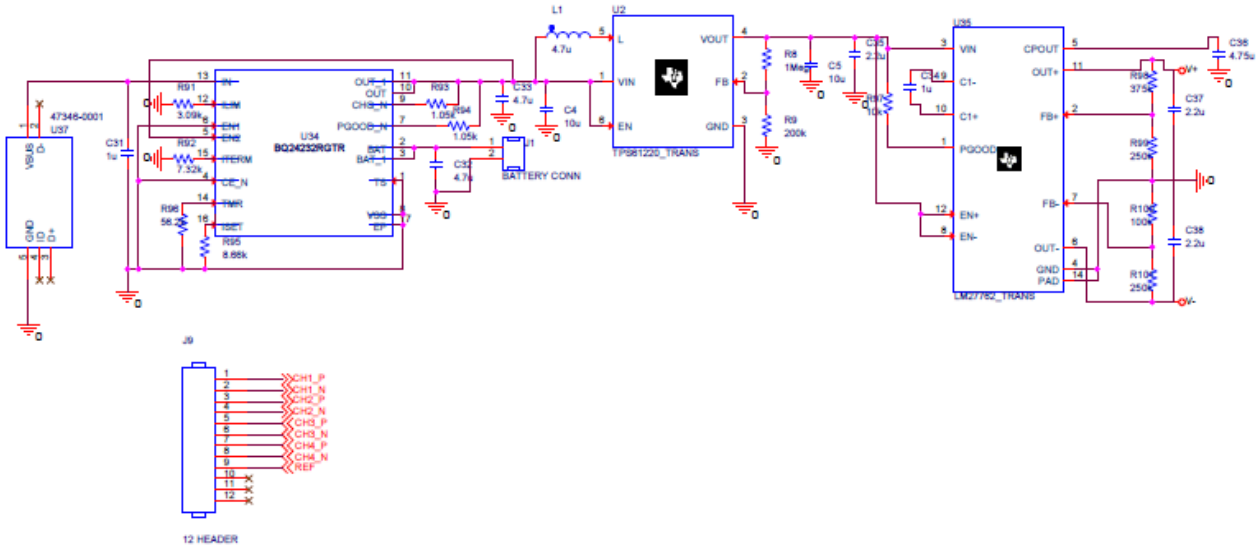

Figure 7. Power supply schematic

2.2. Gateway

The data arrives at the gateway via Bluetooth, controlled by a listening application made using Dotnet core five technology that will manage the sending to the cloud through local rescue mechanisms and retry if the Internet is unavailable. The installed operating system is Ubuntu 20.04.1 server with Bluetooth libraries, net 5. The Raspberry Pi 4 has built-in WIFI and Bluetooth, making it useful for our purposes.

According to cybersecurity best practices, the system is hardened and secured: firewall, anti-DDoS, and SELinux.

SELinux mainly consists of a series of enhancements related to the security of the Linux system, implemented using a mandatory access control architecture and incorporated into the major subsystems of the kernel. It runs directly in the kernel, thus implementing a Mandatory Access Control system. In SELinux, mechanisms capable of separating in-formation are provided precisely based on confidentiality and data integrity requirements, two of the fundamental aspects of what is defined as computer security. The configuration and administration of SElinux is a highly complicated activity. To configure SELinux, the operating system kernel was recompiled.

An in-depth study was devoted to the firewall and mitigating DDOS attacks. In the following paragraph, some de-tails about these security mechanisms are described. Iptables is a powerful firewall built into the Linux kernel and part of the Netfilter project. The DoS, i.e., Denial of Service, aims to flood the resources of a computer system that provides a particular service to connected computers. Iptables can filter specific packets, block sources or destination ports and IP addresses, forward packets via NAT, and many others. It is most commonly used to block destination ports and source IP addresses. When used correctly, iptables is a potent tool that can stop many DDoS attacks. A series of rules have been studied that allow the system to be robust to attacks.

A VPN (Virtual Private Network) allows the creation of a virtual private network that guarantees privacy, anonymity, and data security through a reserved communication channel between devices that do not necessarily have to be connected to the same LAN. For example, the configuration app can be connected to the Raspberry access point and safely access the configuration functions through an OpenVPN connection. The certificate is issued only to authorized persons.

2.2.1. Kernel Recompilation Steps to Enable SELinux (Ubuntu 20.04.2 over PI4)

The first step requires a memory card of at least 32GB and Ubuntu Server 20.04 download, install, and update for Raspberry Pi4 (preinstalled image):

```
launch the controls with sudo
uncomment in file /etc/apt/sources.list:

#sudo vi/etc/apt/sources.list
deb-src http://ports.ubuntu.com/ubuntu-ports focal main restricted
deb-src http://ports.ubuntu.com/ubuntu-ports focal-updates main restricted
#sudo apt update
#sudo reboot
#sudo apt-get build-dep linux linux-image-$(uname -r)
download about 1GB
#sudo apt install libncurses-dev Linux-tools-common fakeroot
```

During the next step, it is necessary to download the kernel repository and compile it:

```
#mkdir ~/kbuild
#cd~/kbuild
#git clone –depth=1 git://git.launchpad.net/~ubuntu-kernel/ubuntu/+source/linux-raspi/+git/focal
```

To customize the kernel, it is necessary to edit, under Debian.raspi/config/, the file:

```
/home/ubuntu/kbuild/focal/Debian.raspi/config/config.common.Ubuntu
```

The file that is generated by the kernel editor instead is:

```
/home/ubuntu/kbuild/focal/debian/build/build-raspi/.config
```

The configuration parameters are:

```
CONFIG_DEFAULT_SECURITY="selinux"
CONFIG_DEFAULT_SECURITY_SELINUX=y
```

The other Selinux parameters are:

```
CONFIG_SECURITY_SELINUX=y
CONFIG_SECURITY_SELINUX_AVC_STATS=y
CONFIG_SECURITY_SELINUX_BOOTPARAM_VALUE=y
CONFIG_SECURITY_SELINUX_CHECKREQPROT_VALUE=1
CONFIG_SECURITY_SELINUX_DEVELOP=y
```

In addition, comments on APPARMOR configurations parameters are:

```
#CONFIG_SECURITY_APPARMOR=y
# CONFIG_SECURITY_APPARMOR_DEBUG is not set
#CONFIG_SECURITY_APPARMOR_HASH=y
#CONFIG_SECURITY_APPARMOR_HASH_DEFAULT=y
#CONFIG_DEFAULT_SECURITY_APPARMOR=y
```

Kernel build can initially take many hours and creates 7 .deb files in ~/kbuild.

```
#cd~/kbuild/focal
#sudo fakeroot Debian/rules clean
#sudo fakeroot debian/rules binary-headers binary binary-perarch
AppArmor support (SECURITY_APPARMOR) [N/y/?] (NEW) N
```

After the kernel build was complete and before the new kernel was installed, the alternate security system apparmor was uninstalled since it conflicts with SELinux:

```
#sudo apt-get remove apparmor
```

To uninstall apparmor and its dependencies:

```
#sudo apt-get remove –auto-remove apparmor
# sudo apt purge apparmor
```

To install the new kernel:

```
#cd~/kbuild
#sudo dpkg -i*.deb
#sudo sync;
```

Pin to SELinux boot for start

```
selinux=1 security=selinux audit=1
```

to file

```
/boot/firmware/cmdline.txt"
net.ifnames=0 dwc_otg.lpm_enable=0 console=serial0,115200 console=tty1 root=LABEL=writable rootfstype=ext4 elevator=deadline rootwait fixrtc selinux=1 security=selinux audit=1
#sudo touch /.autorelabel
```

To install SELinux management packages:

```
#sudo apt install policycoreutils selinux-utils selinux-basics
#sudo apt-get update -y
#sudo apt-get install -yauditd
#sudo apt-get install selinux-policy-default
```

Default Selinux is configured in permissive mode (everything denied is tracked in the logs). It is then possible to generate the rules to be compiled.

```
#sudo selinux-activate
```

In /etc/selinux/config file, by default:

```
SELINUX=permissive
```

Finally, it is necessary to restart:

```
#reboot
```

It is required to start in enforcing mode:

```
#sudo selinux-config-enforcing
```

To disable SELinux, in the configuration file `/etc/selinux/configfile` is necessary to change the following line:

```
from:
SELINUX=enforcing
TO:
SELINUX=disabled
#sudo reboot
```

The first restart after SELINUX integration will take at least 10 minutes to accept ssh connections.

The following command displays the status of SELinux:

```
#sestatus
```

rebuild procedure –

```
#cd~/kbuild/focal
#sudo rm -rf debian/stamps/stamp-build/*
#sudo rm -rf Debian/linux-libc-dev/usr/include/arm-linux-gnueabihf
#sudo rm -rf debian/linux-libc-dev/usr/include/arm-linux-gnueabihf
#sudo rm -rf debian/build/build-raspi
#sudo rm -rf debian/linux-libc-dev/usr/include/aarch64-linux-gnu
#sudo fakeroot debian/rules clean
#sudo fakeroot Debian/rules binary binary-perarch
```

To check if a parameter is set in the kernel:

```
grep -i selinux/boot/config-5.4.0-1034-raspi
```

After installing all the software, a web server is needed, and running the system in permissive mode; then, the rules can be generated automatically.

```
#cat /var/log/audit/audit.log|audit2allow -R
```

An output example is:

```
#============= bluetooth_t ==============
allow bluetooth_t self:alg_socket { bind create };
allow bluetooth_t self:bluetooth_socket { accept bind create getattr getopt listen read setopt write };
allow bluetooth_t self:capability sys_module;
bluetooth_dbus_chat(bluetooth_t)
dev_rw_generic_chr_files(bluetooth_t)
```

The rules that need to be generated can be displayed (in permissive mode).

If the following error appears:

```
audit2allow could not open interface info [/var/lib/sepolgen/interface_info]
```

It is necessary to launch the command:

```
#sudo sepolgen-ifgen
#sudo cat/var/log/audit/audit.log|audit2allow -MRegoleModuloStart
```

To load the rules:

```
#sudo semodule -iRegoleModuloStart.pp
```

To persist in the rules:

```
#semanage fcontext -C -l
```

After including the necessary rules (assuming the rules are allowed), it is likely that the action that has been taken still needs to be completed. It simply fails at another stage, which it could not reach before. As long as previous AVC denials are available in audit logs, regenerate the policy and continue. After all, audit2allow will consider all the AVC denials it encountered, even those that were present before the new policy was uploaded. It is necessary to repeat the operation until nothing more is found.

```
#sudo cat/dev/null>/var/log/audit/audit.log
#sudo reboot
```

Reapply the procedure.

3. Results

The vulnerability assessment identifies, quantifies, and prioritizes a system's vulnerabilities. The article evaluated exposures with a well-known tool: Nessus (Commercial Product by Tenable® [27]). This tool will allow us to assess the system's level of security before (TEST 1) and after (TEST 2) the hardening of the system.

3.1. Vulnerability Assessment Pre-Hardening

The system's initial condition is as the image installs with an IP assigned on the ethernet card and onboard the biomedical software that interfaces with the sensors called Simple Hub. The Nessus tool allows a series of plugins rep-resenting the types of scans that can be carried out. The selection of “Advanced Scanning” is considered.

In the test, the password of the ubuntu non-root user will be provided so that the tool can also test the escalation of root users and identify any internal and not only external vulnerabilities through the network scan.

TEST 1: The test is only the operating system on board the Simple Hub software developed with Microsoft. Netcore technology and Bluetooth Libraries BlueZ.

The system has no vulnerabilities; only info (Tips) represents information that is sometimes important for hackers (Figure 9). Such info is not vulnerable, but it shouldn't be there.

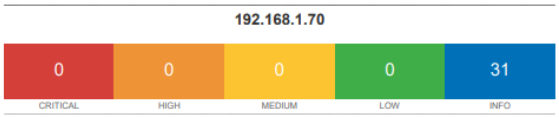

Figure 9. Test 1

The system is already secure but must be prepared at the system level for any future vulnerabilities unknown to date and capable of resisting DDoS (Distributed Denial-of-Service) attacks. In the field of cybersecurity, DDoS attacks indicate a malfunction due to a cyberattack in which the resources of a computer system that provides a service to clients are

deliberately exhausted, such as a website on a web server, until it is no longer able to deliver the service to requesting clients. SElinux ensures that even if an attacker could log in via ssh with brute force attacks with non-root users or through application bugs, he could not take control of the root but remain confined to the SELinux sandbox. DDoS at-tacks can be mitigated by configuring special rules of the Linux firewall "iptables." The Hub will be transformed into a WIFI access point for connecting the management app, then exposed to possible attacks. We can still lower the risk by allowing only packets from the ethernet network connected to the internet router and accepting incoming connections on the WIFI ports 22(ssh) and 4243(TCP server) via VPN.

Installing an OpenVPN server that accepts connections only after authentication (username and password) and certificate is necessary. All this leads to pushing the hardening of the system that lowers the risk of intrusion and then tampering and data theft. It is important to note that Simple Hub is also securely connected to the cloud for pre-processing sensor acquisition data and sending it for historicization in the cloud.

3.2. Vulnerability Assessment Post Hardening

Nessus tool was used to evaluate the system's security level after the hardening of the system and performed the additional test (TEST 2).

The test is carried out with SELinux enabled and firewall enabled and without VPN with the Raspberry trans-formed into a WIFI hotspot, providing an account to the tool to connect and then simulate unauthorized non-root access (phase A).

The test shows that a medium-sized vulnerability is present (Figure 10).

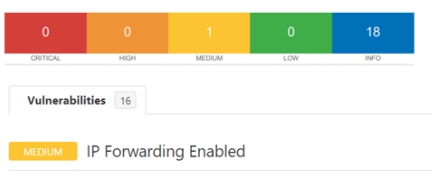

Figure 10: Test 2 (phase A)

That we can consider a false positive as we forward IP packets from WIFI to the ethernet card so those connected via VPN can also access the internet from the Raspberry access point.

We do not provide any accounts, and we can use firewalls and SElinux without VPNs (phase B). We have obtained the results reported in Figure 11.

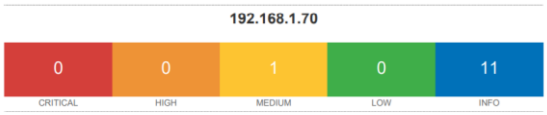

Figure 11. Test 2 (phase B)

As the last test, we enable ethernet only outbound by firewall rule to allow internet access to the HUB and allow connections to ports 22 and 4242 only after establishing a VPN session with a certificate, username, and password on the Wi-Fi connection (phase C). It is important to note that the RASPBERRY HUB has been transformed into an access point to allow the app to configure sensors from the HUB.

In this case, doing the test via WIFI, which is the riskier surface of attack, we obtained the results illustrated in Figure 12.

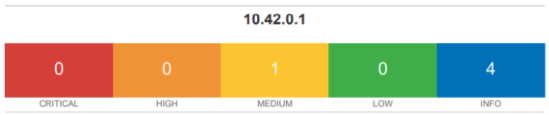

Figure 12. Test 2 (phase C)

We have minimized the information available. The goal is to bring that information to zero. The final report is re-ported in Figure 13.

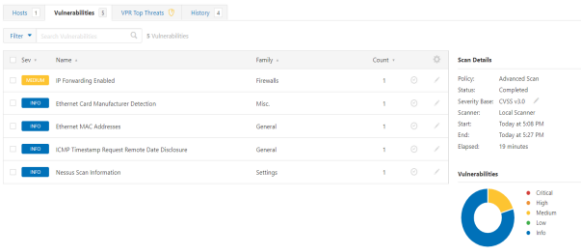

Figure 13. Final report

4. Conclusion

This paper presents a high-performance, secure, wearable, and portable device for biopotential measurement and processing. More specifically, the

system was designed to (i) monitor physical activity in medical and clinical rehabilitation, (ii) evaluate the subject's movements in sports environments, and (iii) monitor wellness indicators. The use of Linux systems in the telemedicine field requires greater attention to cybersecurity. It is necessary to adopt security mechanisms to defend against threats of unauthorized access to the data health of patients through the tampering of the devices themselves. SELinux makes the system safer even if it is difficult to install and configure. Along with an exemplary firewall configuration and hardening system, it is possible to reduce the risk of DDoS attacks and intrusions.

Acknowledgments

This work has been funded by the SIMpLE (Smart solutIons for health Monitoring and independent mobiLity for Elderly and disable people) project (Cod. SIN_00031—CUP B69G14000180008), a Smart Cities and Communities and Social Innovation project, funded by the Italian Ministry of Research and Education (MIUR).

References

1- J. Passos *et al.*, "Wearables and Internet of Things (IoT) Technologies for Fitness Assessment: A Systematic Review." (in eng), *Sensors (Basel, Switzerland)*, Vol. 21 (No. 16), Aug 11 (2021).

2- Wenbin Sun *et al.*, "A Review of Recent Advances in Vital Signals Monitoring of Sports and Health via Flexible Wearable Sensors." *Sensors*, Vol. 22 (No. 20), p. 7784, (2022).

3- G. Yang *et al.*, "IoT-Based Remote Pain Monitoring System: From Device to Cloud Platform." (in eng), *IEEE J Biomed Health Inform*, Vol. 22 (No. 6), pp. 1711-19, Nov (2018).

4- K. Katzis, L. Berbakov, G. Gardašević, and O. Šveljo, "Breaking Barriers in Emerging Biomedical Applications." (in eng), *Entropy (Basel)*, Vol. 24 (No. 2), Jan 31 (2022).

5- H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis." (in eng), *Sensors (Basel, Switzerland)*, Vol. 20 (No. 13), Jun 28 (2020).

6- G. Fortino, A. Guerrieri, P. Pace, C. Savaglio, and G. Spezzano, "IoT Platforms and Security: An Analysis of the Leading Industrial/Commercial Solutions." (in eng), *Sensors (Basel, Switzerland)*, Vol. 22 (No. 6), Mar 11 (2022).

7- Arrigo Palumbo, Patrizia Vizza, Barbara Calabrese, and Nicola Ielpo, "Biopotential Signal Monitoring Systems in Rehabilitation: A Review." *Sensors*, Vol. 21 (No. 21), p. 7172, (2021).

8- Lucas Medeiros Souza do Nascimento, Lucas Vacilotto Bonfati, Melissa La Banca Freitas, José Jair Alves Mendes Junior, Hugo Valadares Siqueira, and Sergio Luiz Stevan, "Sensors and Systems for Physical Rehabilitation and Health Monitoring—A Review." *Sensors*, Vol. 20 (No. 15), p. 4063, (2020).

9- S. Zhao *et al.*, "Wearable Physiological Monitoring System Based on Electrocardiography and Electromyography for Upper Limb Rehabilitation Training." (in eng), *Sensors (Basel, Switzerland)*, Vol. 20 (No. 17), Aug 28 (2020).

10- C. Wu, Y. Yan, Q. Cao, F. Fei, D. Yang, and A. Song, "A Low Cost Surface EMG Sensor Network for Hand Motion Recognition." in *2018 IEEE 1st International Conference on Micro/Nano Sensors for AI, Healthcare, and Robotics (NSENS)*, (2018), pp. 35-39.

11- T. Uktveris and V. Jusas, "Development of a Modular Board for EEG Signal Acquisition." (in eng), *Sensors (Basel, Switzerland)*, Vol. 18 (No. 7), Jul 3 (2018).

12- J. Mangal, "A Smart Wear based Portable Health Monitoring System." in *2020 IEEE International Students' Conference on Electrical,Electronics and Computer Science (SCEECS)*, (2020), pp. 1-6.

13- Mohammed Al-khafajiy *et al.*, "Remote health monitoring of elderly through wearable sensors." *Multimedia Tools and Applications*, Vol. 78 (No. 17), pp. 24681-706, 2019/09/01 (2019).

14- A. B. Jani, R. Bagree, and A. K. Roy, "Design of a low-power, low-cost ECG & EMG sensor for wearable biometric and medical application." in *2017 IEEE SENSORS*, (2017), pp. 1-3.

15- Thanh Chau Nguyen, Tri-Quang Huynh, Tri-Thong Vo, Phuong Nam Nguyen, and Toi Vo Van, "An EEG Front-End System Using ADS1299." Singapore, (2018): *Springer Singapore*, pp. 717-22.

16- Arrigo Palumbo *et al.*, "SIMpLE: A Mobile Cloud-Based System for Health Monitoring of People with ALS." *Sensors*, Vol. 21 (No. 21), p. 7239, (2021).

17- A. Palumbo, B. Calabrese, N. Ielpo, A. Demeco, A. Ammendolia, and D. Corchiola, "Cloud-based biomedical system for remote monitoring of ALS patients." in *2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, (2020), pp. 1469-76.

18- A. Demeco *et al.*, "Quantitative analysis of movements in facial nerve palsy with surface electromyography and kinematic analysis." *Journal of Electromyography and Kinesiology*, Vol. 56p. 102485, 2021/02/01/ (2021).

19- [Online]. Available: https://www.ti.com/product/INA126

20- [Online] Available: https://www.ti.com/lit/ds/symlink/ads1296r.pdf

21- [Online]. Available: https://www.ti.com/product/CC2640

22- [Online]. Available: https://developer.arm.com/Processors/Cortex-M3

23- [Online]. Available: https://www.szrfstar.com/product/144-en.html

24- [Online]. Available: https://www.ti.com/lit/ds/symlink/cc2640r2f.pdf?ts=1668003551888&ref_url=https%253A%252F%252Fwww.google.com%252F

25- [Online]. Available: https://www.ti.com/product/TPS61220

26- Alessandro de Sire *et al.*, "Anterior Cruciate Ligament Injury Prevention Exercises: Could a Neuromuscular Warm-Up Improve Muscle Pre-Activation before a Soccer Game? A Proof-of-Principle Study on Professional Football Players." *Applied Sciences*, Vol. 11 (No. 11), p. 4958, (2021).

27- [Online]. Available: https://www.tenable.com/products/nessus

28- [Online]. Available: https://www.ti.com/product/BQ24232