Expert Systems With Applications 238 (2024) 122285

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

Enhancing workplace safety: A flexible approach for personal protective equipment monitoring

Alessia Pisu [a], Nicola Elia [b], Livio Pompianu [a,*], Francesco Barchi [b], Andrea Acquaviva [b], Salvatore Carta [a]

[a] University of Cagliari, Via Ospedale 72, 09124, Cagliari, Italy
[b] University of Bologna, Viale del Risorgimento 2, 40136, Bologna, Italy

ARTICLE INFO

Keywords:
Artificial intelligence of things
Machine learning
Real-time monitoring
Work safety

ABSTRACT

Workplace safety is a prominent concern, motivating researchers across diverse disciplines to investigate valuable ways to address its challenges. However, creating an efficient system to address this issue remains a significant challenge. Since many accidents happen due to improper usage or complete removal of Personal Protective Equipment (PPE), one straightforward method for enhancing workplace security involves monitoring their usage This paper introduces an Operator Area Network (OAN) system which improves the existing solutions by increasing portability across different users and environments, non-intrusiveness and privacy. To enhance robustness in detecting the situations in which PPEs are not used correctly, we take advantage of Machine Learning to analyse the received signal strength indicator (RSSI) between PPEs in the same OAN The novelty of this work is that it does not exploit RSSI as a proxy of the distance but instead recognizes a signature of the correct wearing of the PPE By employing this system, employers can effectively ensure the proper usage of PPE devices at their worksites while also minimizing any adverse effects on workers' comfort and reducing the setup burden for employers. The system runs a Support Vector Machine (SVM) model several times per second and employs a post-processing algorithm to enhance its initial accuracy further As a result, the system effectively reduces false positives by about 80% and swiftly detects instances of improper usage of the worker's PPE, raising the alarm in less than seven seconds. Moreover, the post-processing algorithm can be customized to meet the specific needs of different use cases, allowing for a flexible trade-off between the detection time interval and the overall accuracy of the detection system.

1. Introduction

Ensuring workers' well-being, health and work performance requires appropriate working conditions and organizational structures (Davidescu et al., 2020). Specifically, safe and hygienic working conditions significantly impact both work quality and life outside the workplace (Greubel et al., 2016; Haar et al., 2014). Various legislation and initiatives reinforce these aspects, including the European Parliament Resolution of 10 March 2022 on a new EU strategic framework for health and safety at work after 2020. Despite these efforts, workplace safety remains a substantial challenge in modern society, as evidenced by statistics on workplace accidents (Eurostat, 2022). Furthermore, the study exploring disparities in working conditions among European Union member states, employing quantitative methodologies like TOPSIS and K-means (Tutak et al., 2022), underscores the need to focus on improving workplace safety. Addressing variations in working conditions, which encompass the effective utilization of PPE (Personal Protective Equipment), represents a fundamental element of workplace safety. Given the ongoing imperative to ensure workers' health and safety, a clear call exists to investigate novel approaches for monitoring PPE compliance. Embracing advanced monitoring technologies for PPE usage can offer valuable insights into safety protocol adherence, thus empowering organizations and policymakers to make informed decisions to elevate workplace safety standards and safeguard workers' well-being.

Workers are required to wear appropriate PPE as a first line of protection, in order to prevent workplace accidents from causing severe physical harm (Ammad, Alaloul, Saad, & Qureshi, 2021). Despite this, workers often do not comply with the use of PPE for various reasons, such as feeling uncomfortable during activities and lack of awareness (Li, Li, Luo, & Siebert, 2017; Wong, Man, & Chan, 2020).

* Corresponding author.
E-mail addresses: alessia.pisu96@unica.it (A. Pisu), nicola.elia2@unibo.it (N. Elia), livio.pompianu@unica.it (L. Pompianu), francesco.barchi@unibo.it (F. Barchi), andrea.acquaviva@unibo.it (A. Acquaviva), salvatore@unica.it (S. Carta).

https://doi.org/10.1016/j.eswa.2023.122285
Received 4 August 2023; Received in revised form 11 October 2023; Accepted 19 October 2023
Available online 21 October 2023

Manually monitoring the use of PPE is a complex task, and it becomes increasingly difficult as the number of workers or the size of the workspace increases. For these reasons, it is crucial to define techniques for automatically monitoring PPE usage, alerting operators whether they do not use the safety equipment correctly, and reporting hazardous situations. Accordingly, in the last decades, academia and industry proposed various methods and technologies to control the observance of these security measures.

Early approaches proposed the usage of wired sensors to monitor the PPEs (Barro-Torres, Fernández-Caramés, Pérez-Iglesias, & Escudero, 2012), which were not comfortable for the operators. More recent works were based on less invasive solutions, such as checking PPE correct wearing only at the entrance to the workplace (Hayward, van Lopik, & West, 2022; Kelm et al., 2013). However this fails in providing a continuous monitoring during all working hours and in specific dangerous areas. More recent *device-free* methods exploit camera-based solutions to reduce the impact on the operators work (Delhi, Sankarlal, & Thomas, 2020; Gu, Xu, Wang, & Shi, 2019; Wu, Cai, Chen, Wang, & Wang, 2019; Xiong et al., 2022). Nevertheless, this approach presents some relevant drawbacks, like requiring an extensive setup on the worksite in order to provide it with closed-circuit television.

In light of these aspects, to carry out automatic monitoring, it is necessary to achieve numerous, often conflicting goals, such as reducing the impact on workers, maximizing site independence, increasing accuracy in detecting hazardous events, and reducing the number of false alarms. In addition, it is necessary to develop cost-effective technical solutions compatible with current labour safety and privacy regulations since most construction small and medium-sized enterprises face barriers to the digital transformation of their processes due to budget constraints (Yilmaz, Salter, McFarlane, & Schönfuß, 2023). Consequently, monitoring the use of PPE is still an open problem, as evidenced by the growing number of published scientific works (Asadzadeh et al., 2020).

In this research paper, we address the following research questions (RQ): RQ1 — Can the Received Signal Strength Indicator (RSSI) of Bluetooth devices be effectively utilized in monitoring systems for assessing the usage of Personal Protective Equipment (PPE)? RQ2 — Is it feasible to develop a straightforward learning methodology that can readily adapt to diverse application scenarios and detect anomalous conditions in the relative distance between two devices based on the RSSI signal? In order to answer these questions, we propose a cost-effective approach for monitoring PPE usage, which improves the existing solutions by increasing portability across different users and environments, non-intrusiveness and privacy. To achieve this target, we base our solution on an Operator Area Network (OAN) of PPEs equipped with low-cost and low-power Bluetooth Low Energy (BLE) devices. The objective is to detect the correct PPE usage by leveraging the Received Signal Strength Indicator (RSSI). More specifically, we exploit the correlation between the RSSI of all PPEs in the OAN by identifying a signature of the correct wearing of PPEs. RSSI information is directly used to perform detection rather than being used for distance estimation.

To recognize this signature, we use machine learning (ML) to process the input RSSI from PPEs in the same OAN. While an ML approach requires an initial training procedure, it provides the following advantages: (i) It efficiently combines the information from multiple PPEs to recognize not only the proximity of PPE but also its correct usage; (ii) It makes our approach more robust to environmental and operator conditions (e.g. body shape, position, etc.), as well as transceiver orientation.

We explored different machine learning algorithms (i.e. support vector machine, isolation forest, and support vector machine with stochastic gradient descent) deployed to the gateway node (in 3.2 we refer to it as "primary device") that, in the current implementation, is embedded in the operator belt. The processing is thus local to overcome connectivity problems that may be frequent in workplaces and to enforce privacy preservation.

In response to the aforementioned research questions, this article's primary contributions are as follows:

- We define the requirements for a PPE monitoring system that overcomes open challenges in the state of the art, such as being easily configured at the worksite and minimally impacting the work of the operators. Accordingly, we design a system architecture that meets the requirements defined using two types of devices composing the OAN, namely primary and secondary.
- We compare different ML algorithms for processing data of PPEs in the OAN to detect PPE misuse. We find that SVM is the best solution for the considered use case in terms of a trade-off between false positives and false negatives. The resulting model exhibits an accuracy of 88.1% with an F-measure equal to 90.2%. It proved to be effective in various scenarios, such as the different physical characteristics of the operators wearing the PPE devices and different environments.
- We defined and implemented a strategy to let the system designer tune the trade-off between two contrasting requirements: the acceptable number of false positives and the time delay for receiving notifications following a detection event.
- We designed and tested the OAN by applying it to a specific use case involving monitoring the operator's helmet and shoes. Through experimentation, we demonstrated that the method effectively minimizes false positives by accepting a 6-second delay between the operator's helmet removal and the event detection.
- We released a dataset containing data from the RSSI measurements taken from the testing of our subjects placed in the same environmental conditions while performing regular movements. In addition, we release the dataset we use to test the machine learning algorithm (Firmware and dataset repository).
- We released the firmware's source code developed for executing the proposed task on the target IoT devices (Firmware and dataset repository).

The rest of this paper is organized as follows: Section 2 overviews the methods and technologies exploited in the paper and introduces related works. Section 3 presents the system's design. Section 4 describes data collection and processing to implement the proposed algorithms. Section 5 presents the experimental findings. Section 6 discusses the results. Finally, Section 7 concludes the work and discusses future developments for improving our framework.

2. Background and related work

In this section, we present the technical background helpful in understanding the article's content (Section 2.1) and provide an introduction to literature related to our work (Section 2.2).

2.1. Background

Bluetooth Low Energy (BLE) (Heydon & Hunn, 2012) is a Wireless Personal Area Network (WPAN) technology that aims to define a version of Bluetooth that can operate with low energy consumption and detect small amounts of data. In this work, we exploit BLE to decide whether PPEs are realistically worn. More specifically, we exploit the Received Signal Strength Indicator (RSSI) (Wu, Lee, Tseng, Jan, & Chuang, 2008), a measure of radio signal strength calculated in dBm. Since the power varies depending on the proximity to the signal source, the closer the RSSI value is to 0, the smaller the distance between the two devices.

Despite the fact that several factors influence the value of RSSI (such as the multipath effects caused by the reflection and dispersion of radio signals in the environment) (Pu & Chung, 2008), various works develop formulas and techniques for translating RSSI values into distance measurements (Kumar, Reddy, & Varma, 2009; Pascacio, Casteleyn, & Torres-Sospedra, 2021). The state-of-art shows that BLE is widely used for tracking and localization tasks by leveraging the RSSI (for instance, Ji, Li, Zhu, and Liu (2022), Thaljaoui, Val, Nasri,

and Brulin (2015), Wang, Yang, Zhao, Liu, and Cuthbert (2013)). Such works often focus on static conditions, e.g., continually operating in the same indoor environment and using fixed landmarks (anchors), and the combination of body area networks and anchors has already been successfully employed in other industrial use cases, such as studying human processes in manual manufacturing (Pilati & Sbaragli, 2023).

However, in the use case of PPE usage monitoring, many additional dynamic factors affect the RSSI value. The first one, since we are constructing a body area network, is the different physical characteristics of human bodies (Parmar, Kelly, & Berry, 2022). Another factor is the movements performed during work activities (Booranawong, Jindapetch, & Saito, 2018). Finally, various workplaces have different configuration of the environment (walls, physical obstacles, etc.) that affects signal refraction differently.

Consequently, in our context, the RSSI value alone between two IoT devices is insufficient to accurately calculate the distance between them. In order to develop an effective method of evaluating PPE use, it is necessary to construct an approach that considers all the factors mentioned and adjusts for their changes in real time. Obtaining a heuristic that exactly solves the problem is challenging. Accordingly, in this paper, we use machine learning to develop an algorithm able to analyse simultaneously all RSSI values of the same OAN and to determine the correct use of PPE. Other work has already successfully employed artificial intelligence in the RSSI processing (Singh, Choe, & Punmiya, 2021).

2.2. Related work

The scientific literature on PPE monitoring covers different methods and techniques. Earlier, IoT solutions for PPE monitoring used a Body Area Network (BAN) with RFID or cables. For instance, Barro-Torres et al. (2012) required workers to wear a BAN with RFID sensors, ensuring real-time PPE positioning. But this system had cables that hindered mobility. In contrast, our approach allows free movement with BLE communication, removing the need for cables. Sole, Musu, Boi, Giusto, and Popescu (2013) proposed a two-network architecture: a BAN with RFID-tagged PPE and fixed nodes using RFID readers. However, this setup increased costs and time for larger workplaces. Kelm et al. (2013) and Hayward et al. (2022) introduced a smart portal at workplace entrances using RFID tags on PPEs. However, this approach cannot be considered continuous monitoring. Recent developments use real-time cameras and computer vision to detect PPE use. For example, Gu et al. (2019) and Delhi et al. (2020) improved the accuracy of safety-helmet and safety-vests detection using transfer learning and Region-Based Convolutional Neural Networks. These camera-based solutions require prior setup and are susceptible to occlusions and adverse weather. Other works suggest BANs using wireless technology like WiFi and BLE, aligning with our BLE-based approach. Abbasianjahromi and Sohrab Ghazvini (2021) used magnetic sensors, Yang, Yu, Shirowzhan, sepasgozar, and Li (2020) automated PPE-tool coupling alerts, Kim, Wang, Min, and Lee (2018) focused on safety-helmet detection with accelerometers, and Booranawong et al. (2018) tracked humans with RSSI indoors. Some recent works like Campero-Jurado, Márquez-Sánchez, Quintanar-Gómez, Rodríguez, and Corchado (2020) introduced smart helmets for environmental monitoring but did not verify PPE use. In a similar way, Rescio et al. (2023) proposed a wearable system to monitor worker stress, but not PPE use. In the category of active monitoring and personal instrumentation, our approach excels in adaptability, noise handling, scalability, and simplicity. It does not need specialized sensors or complex remote systems and maintains user privacy. Although a quantitative comparison of these works is not possible, we provide a more detailed analysis in Section 6.6.

3. Our proposal

This section describes the solution we propose. First, Section 3.1 identifies the problem requirements. Then, Section 3.2 presents the system design we carry out per the specified requirements. Section 3.3 delves into the design of IoT devices. Finally, Section 3.4 discusses the implementation of our solution.

The architecture as a whole adheres to the principles of the computing continuum, encompassing both cloud and edge components. This design offers notable benefits in terms of enhancing safety measures. By effectively utilizing the computing continuum, the system enables intelligent analysis, thereby facilitating the identification of workplaces or scenarios with a higher frequency of improper PPE usage. This valuable insight empowers organizations to develop targeted safety improvement interventions, effectively mitigating risks and cultivating a safer working environment.

3.1. System requirements

The paper seeks to present a solution for the automated monitoring of Personal Protective Equipment (PPE) usage while minimizing disruption to operators' daily activities and regular work processes. Specifically, we have chosen to focus on monitoring the usage of safety helmets and safety shoes. To attain the stated goal, the solution needs to meet the following specified requirements:

Efficacy The system must be able to recognize when the target PPEs are being worn or not. Achieving this goal requires determining what metrics should be used to assess whether the system can correctly identify usage.

Usability The solution must minimize workers' hindrances; for instance, avoid wearing devices connected through wire networks or large devices that impede workers' movements while performing activities.

Portability The solution must be workplace independent, i.e. it must avoid the need for initial workplace configuration. Workers should have a plug-and-play tool without requiring additional expensive operations that depend on the workplace, such as installing a network of cameras or configuring a network of anchor devices.

Scalability The solution must be able to adapt as the data grows, for example, as the number of operators constituting a work team increases or as the number of teams in the same workplace grows.

Traceability When an alarm occurs, such as failure to use PPE, the system must notify the operator and record the event to allow future analysis of the work session.

Privacy-preserving The solution should be limited to collecting the minimum data essential to achieve the project goal (i.e., verifying PPE use) without collecting additional data on the worker. It is crucial to find the balance between security supervision and respect for the worker's privacy.

3.2. System architecture

This section describes the system design process: Fig. 1 and shows the general architecture of our system: we detail each architecture component below.

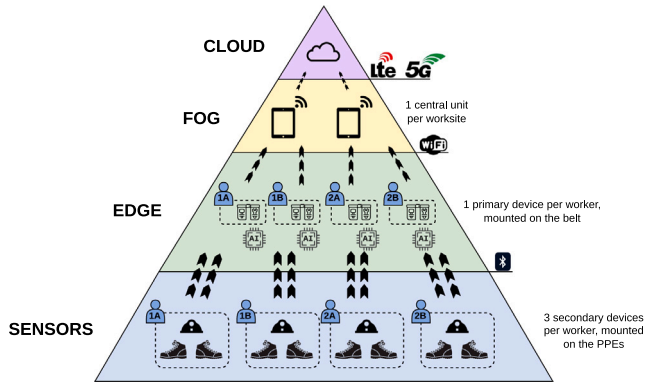


Fig. 1. Hierarchical Architecture of the IoT System. This diagram illustrates a layered structure wherein the base consists of numerous sensors responsible for collecting and transmitting substantial volumes of data. These data are then forwarded to the layer above, which represents edge devices. The edge devices, in turn, process the data and transmit a refined dataset to the subsequent layer: fog layer. The latter is responsible for orchestrating the operations of the edge devices and transmits only essential data to the apex of the hierarchy, symbolizing the cloud.

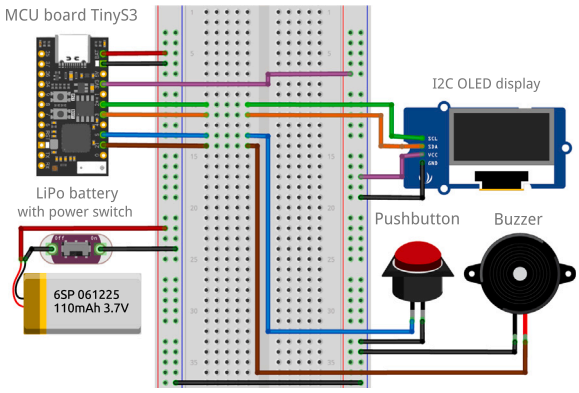


Fig. 2. Schematic of the primary node device prototype.

Sensors Layer The bottom layer of our architecture is responsible for identifying workers' PPEs and collecting the necessary data for monitoring. This layer comprises some IoT devices we develop, which we define as *secondary devices* and are placed on each PPE. Each worker wears three secondary devices (thus three sensors), which are placed, respectively, on the helmet and on each shoe. These devices are connected by means of Bluetooth Low-Energy to a device of the edge level. Cable-free communication and small devices contribute to achieving our *Usability* requirement.

Edge Layer The goals of the edge layer are to process data from the sensors layer, calculate whether PPEs are being worn correctly, and communicate related events both to the operator and remotely. This layer comprises an IoT device we develop, which we define as *primary device* and is placed on the worker's belt. We decided to set the primary device on the belt for several reasons. First, the workers are more likely to remove their helmets or shoes than their work belts. In addition, the belt is more suitable for hosting a bigger edge device than other PPEs and, due to its position in the human body, can easily accommodate user interaction tools such as displays or buzzers. The primary device collects RSSI values that measure the signal strength of its associated secondary devices (i.e., helmet and operator's shoes). Then, through our algorithm, it determines whether the devices are worn correctly. More specifically, in order to achieve our first requirement, *Efficacy*, we develop an AI-based algorithm that mitigates signal errors and processes the signals of all secondary devices in a combined manner. We deeply describe our algorithm in Section 3.4. The primary device continuously detects secondary ones, thus producing the system's raw data. At the same time, it runs the system's business logic locally, producing an output that requires much less bandwidth to be transmitted rather than transmitting raw data. It is worth noting that the reduction of the amount of data propagated through the different layers also lowers the burden on communication modules, reducing their power consumption. While reducing the amount of data exchanged between upper layers, the edge layer also prevents propagating privacy-sensitive data from the secondary nodes upwards. Our design choices aim to meet the requirements of *Scalability* and *Privacy-preserving*.

Fog Layer Since a workplace generally involves several workers, the goal of the layer is to act as a bridge between the workers and the cloud. The fog layer is responsible for collecting the messages it receives from each worker's primary device and sending them to the cloud. This layer comprises a device we define as a *central unit* placed in the work site. In this way, the primary devices do not have a load of transmitting data to the cloud, so it is possible to reduce their components, consumption and size. Each edge device communicates with the central unit by means of a WiFi connection, avoiding cabled communication in the worksite and achieving the *Portability* requirement.

Cloud Layer The cloud layer aims to collect field-generated events and save them permanently, providing a comprehensive view of workplace data as required by the *Traceability* requirement. In this way, the system enables intelligent analysis aimed at improving safety. For example, it is possible to identify whether there are any workplaces or situations where there is a higher frequency of incorrect PPE use and design safety improvement interventions.

3.3. Device design

Within the designed architecture, this work also designs, develops, and tests the primary and secondary devices and the AI algorithm. In this section, we focus on presenting the design of the primary nodes (Edge layer) and secondary nodes (Sensors layer).

We design two types of IoT devices which we call, respectively, *primary* and *secondary* devices. The secondary devices are low-power devices attached to the PPEs to be monitored: precisely, we mount one IoT device to each PPE. The primary device collects information from the secondary devices, processes it, communicates with the operator, and shares it with the remote components. Accordingly, there is only one primary device for each operator. We deploy our primary device on the safety belt and the secondary devices on the helmet and protective shoes. In particular, the selected PPEs become IoT nodes by means of the application of an IoT device on top of them. As a result, four IoT nodes form the Body Area Network (BAN) of each worker. Given the peculiarities of primary and secondary devices, they differ both in hardware and software components.

Hardware We design two slightly different prototypes for the two types of nodes. Each prototype has a lithium battery with a charging circuit, so it can be recharged when the device is not worn and ensure sufficient autonomy of use. Moreover, we select small devices so they are light enough and do not cause problems in daily tasks. Both prototypes use TinyS3, a development board incorporating the ESP32-S3, a Bluetooth 5 module with Bluetooth Low Energy + Mesh, a 2.4 GHz WiFi module, a USB-C connector and a low-power RGB LED. Considering the

test scenario of operators at work, the two prototypes differ in achieving different purposes in the BAN. The primary node must be capable of communicating messages to the worker wearing it to warn him of situations in which he is not wearing the protective equipment correctly. For this reason, the prototype of the primary node, which we illustrate in Fig. 2, includes a small OLED display and a buzzer that can easily communicate visually and audibly with the user. Although our use case does not involve the operator using hearing-restrictive PPE, we highlight that alarms are currently notified by sound and as a visual message on the OLED screen. Moreover, extending the IoT device to include alternative signalling mechanisms is possible. These alternatives may include vibrators, vibrating bracelets, or more conspicuous flashing lights to ensure effective communication. In addition, it must have a button to switch off the alarm that warns of a dangerous situation. On the other hand, the secondary device prototype is more basic and only possesses the battery, charging circuit and TinyS3. Indeed, since this type of device must be applied to PPEs, we minimize its size to reduce its impact on operators.

Firmware We evaluate different protocols and processors for design and prototype development to identify which suits the specific project requirements best. In order to realize this vision, we choose two communication protocols: WiFi and BLE. We choose BLE for the detection of secondary devices by the primary node. This technology saves energy while providing enough range and a good broadcasting frequency. We exploit WiFi for sending data from the primary node to the backend, allowing sending data efficiently and with a more extensive range than others. Therefore, the hardware we choose simultaneously allows the use of BLE and WiFi while running the business logic that governs the generation of events. On the other hand, the backend can be any system able to act as a WiFi gateway for receiving data from primary nodes.

AI Software As previously explained, the business logic behind the emission of PPE-related events relies on the RSSI signals acquired from secondary nodes by the primary node. We integrate machine learning algorithms because it is challenging to predict all situations in which a device is worn incorrectly or not at all, as RSSI values can vary due to different factors. In the system we propose, the execution of machine learning algorithms occurs in the primary device (thus at the edge level), which calculates the RSSI value of all secondary devices. Moreover, running the algorithm at that level avoids transmitting real-time data to the higher layers, mitigating problems such as poor connectivity, service delays, and privacy leakage vulnerabilities.

3.4. Implementation

In this section, we discuss the hardware and software components developed to implement the proposed system.

In order to meet all the PPE nodes requirements, we choose to use the Unexpected Maker's TinyS3 development board, which is built around the ESP32-S3 System On Chip (SoC) (ESP, 2023). The ESP32-S3 SoC supports Bluetooth Low Energy 5.0 (BLE) and implements a high-gain 3D ceramic antenna. Thanks to its characteristics, our hardware can transmit Bluetooth packets with an advertisement interval of only 20 ms, with a throughput of 50 packets per second. Fig. 4 represents the prototypes we develop: on the right is shown the primary node, and on the left is the secondary one.

The software environment on top of which we build the firmware is MicroPython (mic, 2023). MicroPython is a Python interpreter and runtime that runs bare-metal on different supported families of microcontrollers. As a consequence, the source code written for MicroPython can be interpreted by any supported hardware platform. Our strategy for designing the firmware is based on the concurrent execution of coroutines. At a higher level, the primary node works by looping between the following steps: (i) acquire broadcast data, (ii) estimate the RSSI of secondary node links, (iii) process this data to generate alerts when a PPE removal event occurs. Algorithm 1 illustrates the process that is performed within the primary node.

Algorithm 1 Primary device loop

```
alarms_count ← 0
alarms_threshold ← 10
loop
    he ← RSSI signal from helmet device
    ls ← RSSI signal from right shoe device
    rs ← RSSI signal from left shoe device
    input_array ← compute_input_features(he, ls, rs)
    result ← run_model(input_features)
    if result is False & alarms_count ≥ 0 then
        alarms_count = alarms_count + 1
        if alarms_count ≥ alarms_threshold then
            emit an alarm towards the user interface
            emit an alarm towards the central unit
            wait for user input
            alarms_count ← 0
            continue
        end if
    else if result is True & alarms_count = 0 then
        continue
    else if result is True & alarms_count > 0 then
        alarms_count ← 0
        continue
    end if
end loop
```

The algorithm combines a machine learning algorithm and a control mechanism. First, the RSSI values of the secondary nodes (helmet, right shoe and left shoe) are estimated and stored in raw buffers. Next, they are pre-processed to provide the equivalent of 5-second moving windows of meaningful aggregated objects (shoes, helmet). The resulting data is used in the processing phase to feed the machine learning algorithm, which is responsible for detecting whether the situation in which the operator finds himself is anomalous or not. Afterwards, the post-processing algorithm checks whether the abnormal condition is long enough to determine an actual moment of danger to the worker using a threshold. If the situation is dangerous, an alarm is sent towards the user interface (i.e. display message, buzzer) and to the fog layer.

The MicroPython ecosystem includes a standard library, which implements compatible versions of modules from the Python Standard Library, and specific packages that do not have equivalents in other Python environments. The latter include drivers for hardware peripherals and libraries to enable embedded functionalities such as Bluetooth communication.

It is worth noting that the Bluetooth functionalities needed to build this project are provided by the *aioble* library, an object-oriented asynchronous wrapper for the Bluetooth API. At the time of writing this paper, the main ESP32-S3 MicroPython build uses the Espressif ESP-IDF framework to run MicroPython as a task under FreeRTOS. More in detail, MicroPython is run as a task pinned to Core 1, while the WiFi and Bluetooth controllers are run as tasks pinned to Core 0. This allows the aioble library to work parallel to the user application. From our perspective as firmware developers, the result is that the BLE scanner can be coded as an asynchronous generator that yields the scan results and that is constantly populated in the background. Therefore, we can make use of all the CPU time to execute application tasks rather than having to leave CPU time to execute the BLE controller.

If the BLE scan was a task pinned to the same core of the application, we would have needed to maximize its execution time in order to

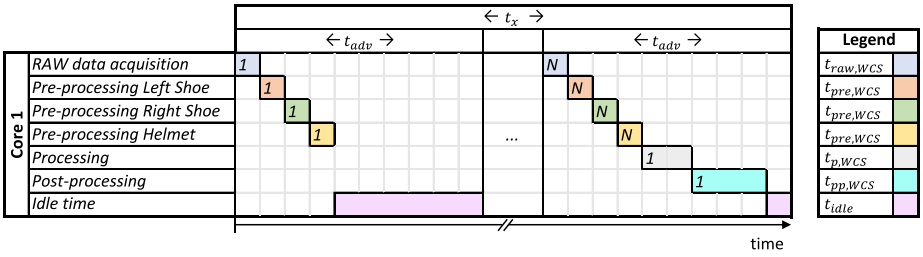


Fig. 3. Graph representing the worst-case scheduling of coroutines on Core 1. The number inside each scheduled coroutine represent its execution cardinality inside the processing execution interval t_x.

maximize the probability of intercepting the broadcast messages of the PPE devices in advertising mode.

The *uasyncio* library that we used to manage concurrent coroutines will therefore run these coroutines on the Core 1. Then, their execution times must fit the firmware's timing to run the data processing. The pre-processing task described earlier must be run every time new RAW data is collected because the data structures are designed to avoid storing long data sequences. Its execution frequency will then be, in the WCS (Worst Case Scenario), equal to the RAW data acquisition frequency. The processing task must be run according to the frequency at which the AI model has to be run. The post-processing will follow the processing task.

In our case, we recall that the PPE devices are three, $N_{\text{dev}} = 3$, and they are configured to provide an advertising interval equal to $t_{\text{adv}} = 100$ ms. The incoming data from these devices must always be pre-processed. Our tests demonstrated that the pre-processing time of any PPE device, when considering $t_{\text{w}} = 5$ s time windows, requires at most $t_{\text{pre,WCS}} = 4.2$ ms. On the other hand, the processing and post-processing WCS times are respectively: $t_{p,WCS} = 14.5$ ms and $t_{\text{pp,WCS}} = 0.4$ ms. The time required to acquire RAW data from the BLE buffer is always lower than 7 ms, thus $t_{\text{raw,WCS}} = 7$ ms.

Given a wanted processing execution interval t_x, the free CPU time that remains between the intervals is given by the following mathematical expression:

$$t_{\text{free}} = t_{\text{x}} - \frac{t_{\text{x}}}{t_{\text{adv}}} \cdot (t_{\text{raw,WCS}} + N_{\text{dev}} \cdot t_{\text{pre,WCS}} + t_{\text{p,WCS}} + t_{\text{pp,WCS}}) \tag{1}$$

and it is depicted in Fig. 3.

If its value becomes negative, then the system will not be able to process the coroutines in time, leading to an increasing delay in data acquisition. In our case, the wanted processing interval is $t_x = 200$ ms, thus the formula can be resolved as follows:

$$\begin{aligned} t_{\text{free}} &= 200 - \frac{200}{100} \cdot (7 + 3 \cdot 4.2 + 14.5 + 0.4) \\ &= 131 \text{ ms} \end{aligned} \tag{2}$$

Being $t_{free} > 0$, we can state that our system is able to correctly run the defined tasks without leading to any loss of RAW data. It is worth underlying that the parameters that implicitly affect this formula are the advertising interval of the PPE devices and the length of the time window considered to build the data structures. Any increase in one of them will have a negative impact on the remaining free CPU time.

It is also worth noting that, at the time of writing this paper, the MicroPython Bluetooth API does not allow getting an estimated RSSI from a BLE connection. In contrast, it will enable getting this measure from a broadcast reading.

We assembled a prototype employing commercially available components that were not specifically engineered for deployment in extreme environmental conditions, such as extreme temperatures, high humidity, or intense physical stress. According to the proposed monitoring use case, we leveraged plastic housing to make our devices resistant to moderate rain. Moreover, the evaluation boards are built on top of an ESP32-S3R8 chip that operates within ambient temperature ranging from −40 to 65 °C. It is imperative to recognize that the suitability of these components may be contingent upon the specific use case. Therefore, a comprehensive evaluation of these components' resilience to extreme environmental factors and physical stress on the IoT devices is essential to ensure their reliability in challenging operational scenarios. This evaluation entails a careful review of the components' datasheets and may necessitate additional measures, such as the potential sealing of device casings, to bolster their performance and longevity under harsh conditions.

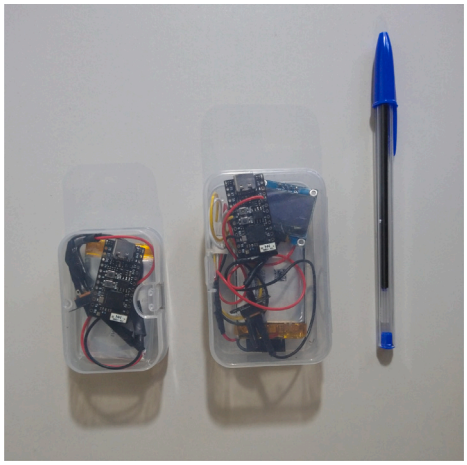


Fig. 4. Picture depicting the primary node device (right) and secondary node device (left), with a ballpoint pen adjacent for size scale reference.

4. Experimental setup

This section presents the strategies used for data collection and processing, as well as the metrics used to evaluate the algorithms. Section 4.1 presents our tests to check the hardware used in data collection; Section 4.2 describes the data collection methodologies. Next, in Section 4.3, we present the method for processing data for the AI algorithm. In Section 4.4 presents the algorithms that we test for the novelty detection approach. Finally, Section 4.5 discusses the evaluation metrics of the selected algorithms.

4.1. Hardware performance

In this section, we present the methodologies we use to validate the performance of our hardware devices. We hereby present several tests we propose to evaluate the behaviour of the chosen hardware devices thoroughly. Indeed, Bluetooth devices' behaviour heavily differs from device to device based on the combination of radio module and antenna. The former implies the support for a certain Bluetooth protocol, thus the support for a set of functionalities and communication protocols, while the latter implies a particular spatial signal coverage and range.

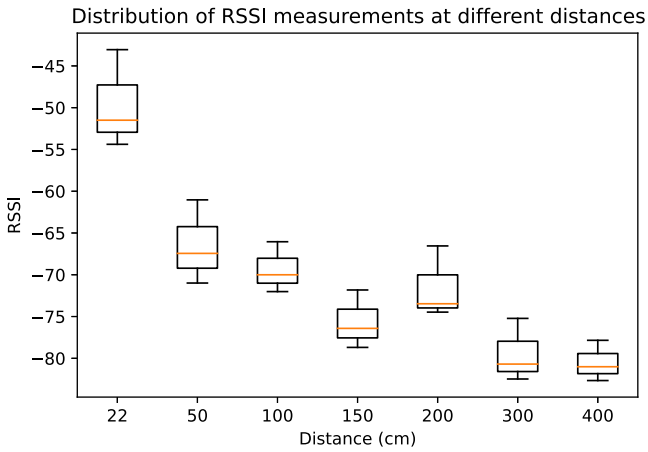


Fig. 5. Distribution of RSSI measurements versus distance between central and peripheral devices. Each boxplot is obtained by averaging 10 min of recorded measures recorded with different instances of the reference board, TinyS3.

The first experiment aims at estimating the RSSI signal variation with respect to the distance between the advertiser and the central. As clarified earlier, our algorithm will not calculate a distance between two objects from their RSSI value because of the many signal disturbance factors that will arise in our use case. However, at this stage, we perform tests on a noise-free plane to understand the basic behaviour of the RSSI signal and make sure that all the devices do not show anomalies. In this regard, we set up a device to act as a Bluetooth advertiser with a 20 ms advertising interval, i.e. sending packets with 50 Hz frequency, and another device to act as a Bluetooth central, which intercepts the broadcast packets and gives an estimation of the signal's RSSI. The two peripherals are always put on the same horizontal plane, with a fixed orientation, in an indoor environment, without obstacles between them. We allow the central device to acquire data for 10 min at each different distance (0.5, 1, 1.5, 3 m) and average it.

Fig. 5 presents the results. The devices present consistent individual behaviours and slight differences between their trends from these data. This experiment leads to the intuition that, since the absolute values of RSSI significantly differ from one device to another, it is convenient for the scopes of this work to consider relative measures, such as the variation from the average of RSSI values detected in a time window.

4.2. Data collection and setup

Once we have tested the proper operation of the devices without interference, as the next step, we organize a data acquisition phase where the devices are worn.

These tests allow us to verify the strength of the intuitions presented in the paper and to develop a system capable of addressing the issues arising from the interference of the human body and the person's surroundings. First, we performed an outdoor test. Then, we repeated the same test in an indoor environment. Below, we describe the test steps, the two settings, and the participants involved.

We design a *circuit* as a precise set of movements and operations and let different people wear our IoT devices in the circuit. In this experiment, we place the devices in the following PPEs: left and right shoes, helmet and work belt. To recognize and be able to distinguish the signature of RSSI values obtained in both conditions of PPEs correctly worn and not, we ask operators at some point in the experiment to put off the helmet.

Each data collection experiment can be split into two main phases:

1. the user wears all the devices correctly;
2. the user removes the helmet and moves away from it;

During the tests, the users are asked to move naturally. Therefore, in each phase, there are moments in which the subject is moving and moments in which he is stationary. As part of the second stage, each participant walks approximately 10 to 20 metres away from the helmet and then continues to move spontaneously. Spontaneous movement is critical because it guarantees the presence of signal variations that would be compatible with a working activity and a realistic example of actual device use, ensuring a representative signature. The data collection sample consisted of thirteen individuals: seven participated in the outdoor experiments, and six participated in the indoor experiments. The experiment's subjects have different physical characteristics, such as height or build, in order to have a more representative sample of people for the test, as shown in Fig. 6.

Operators' survey duration and steps are identical in both the outdoor and indoor tests. The environment and the sample of participants vary between the two tests.

Test 1: Outdoor. The outdoor environment contained side walls and slight radio interference.

Test 2: Indoor. The indoor environment consisted of a room containing numerous sources of noise: more than 15 devices connected using WiFi and BLE; 8 people not involved in the experiment were seated at desks; thick walls, tables, closets, and other furniture.

4.3. Data preprocessing

As a result of the previous experiments, we obtain the RSSI value of each secondary node, which indicates its distance from the primary node. Generally, the higher the RSSI value is, the shorter the distance is. The signal's intensity depends upon the environment in which it is detected, so this information alone cannot be used to determine distance accurately. Consequently, as a next step, we perform preprocessing of the signal data, as described below.

Considering the significant variability of the signal and its susceptibility to interference, we choose to use moving windows for data grouping. The optimal window length can be defined by experimentation, and in our case, we find that a 5-second window makes it possible to eliminate some outliers without losing significant behaviour. It is possible to extrapolate more helpful information for each time window to improve the accuracy of the data. The variance and standard deviation are calculated to represent other useful information. The variance enables us to understand the variability of the data, allowing us to investigate the movement of the mean values. The standard deviation will enable us to summarize the variations from the mean. In general, as distance increases, the number of detections lowers, so we also calculate the number of detections occurring over time. Then, for each temporal window, we compute the following parameters:

Count helmet The number of detections obtained in the current time window. This data is significant because as the distance increases, the number of detections decreases since the signal fades.

Average helmet The moving average of the data collected by the helmet in the current window. This average is made by ignoring null values in order to avoid having drastic variations towards zero each time data is not collected. It is deemed more efficient to encode the information on the empty window by defining the value of the count variable as zero.

Variance helmet The variance is calculated using the moving average of the helmet in the current period.

Standard deviation helmet The standard deviation is calculated on the moving average of the helmet in the current temporal window.

Count shoes The minimum number of detections obtained from a shoe. In this way, significant changes in shoes can be displayed.

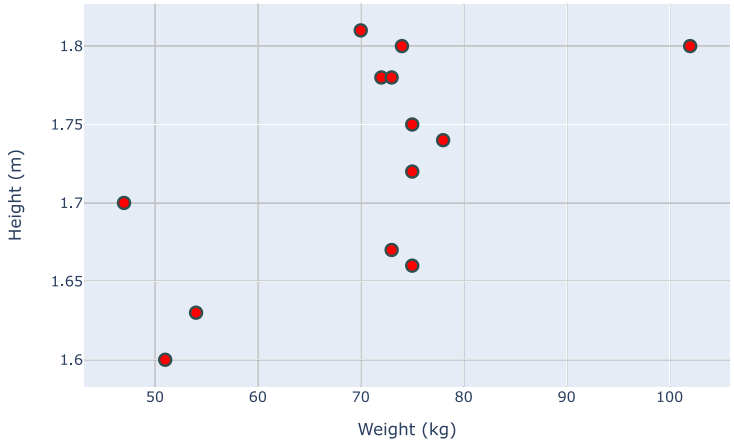


Fig. 6. Physical characteristics of the subjects involved in the experiments.

Average shoes The moving average of the current window is relative to the average values of the two shoes. The average is collected in the same way as the helmet but is calculated from the moving averages of the two shoes.

Variance shoes The variance is determined by the overall moving average of the two shoes relative to the current temporal window.

Standard deviation The standard deviation is calculated on the overall moving average of the two shoes based on the current time frame.

As previously mentioned, we use a single 5s time window to group data and filter out interference caused by the external environment.

We then separate the data collected on the same person so that we can build training and test set. The training set consists of approximately the first minute and a half, while the test set contains roughly the next three minutes of experimentation. In this way, the training set contains only phase 1 and, therefore, only moments where the devices were worn correctly, while the test set consists of part of phase 1 and phase 2, having a combination of moments where the helmet was worn correctly and in a wrong way. We manually label the test set indicating: (1) instances in which the subject is correctly wearing all devices, (−1) instances considered abnormal, indicating times when the helmet is not correctly worn.

4.4. Novelty detection algorithms

Once we have created the datasets, we apply machine learning algorithms. In particular, to address the research problem, we decided to adopt novelty detection algorithms. Novelty detection or outlier detection is a mechanism that identifies events that differ from the rest. Such a model is trained on a set of data that it recognizes as normal behaviour and learns its peculiarities. Afterwards, it is able to distinguish events that are not similar to those on which it is trained. It is particularly effective in domains like the detection of fraudulent bank transactions, anomalous behaviours, etc.

Our approach consists of creating an ad-hoc model for each operator using the devices. By modelling the correct behaviour, which is reached when the operator is wearing every device, we can identify moments of incorrect usage by exploiting a novelty detection approach. This strategy assumes that normal patterns are available in the training set, while abnormal patterns are relatively few and present only in the test set.

We selected three different algorithms: OneClassSVM, Isolation Forest and SGDOneClassSVM. One Class Support Vector Machine (SVM) is a variation of the SVM used for binary classification and novelty detection approaches. It calculates a boundary using the training data, and the new data that lies outside that boundary is classified as an anomaly. OneClassSGDSVM is a Stochastic Gradient Descent (SGD) version of the OneClassSVM. Isolation Forest is a popular algorithm, an ensemble of binary decision trees. It describes the observations with decision trees and assumes that outliers can be found in short paths to leaves, making them easier to isolate.

4.5. Evaluation metrics

This section presents the evaluation metrics used to assess the quality of the results obtained from the artificial intelligence algorithm used to identify events where personal protective equipment is not correctly worn. To evaluate the realized algorithm, we use several metrics to understand better how the algorithm performs. The algorithm recognizes two classes of data: (i) devices are worn correctly; (ii) devices are not worn correctly.

Confusion matrix: the confusion matrix (CM) contains the values of True Positives (TP), False Positives (FP), True Negatives (TN) and False Negative (FN).

$$\mathrm{CM} = \begin{array}{|c|c|}\hline TP & FP \\ \hline FN & TN \\ \hline \end{array} \tag{3}$$

Accuracy: it represents how many correct predictions were made by the algorithm in relation to the total number of predictions. It is expressed by the following formula:

$$a = \frac{TP + TN}{TP + TN + FN + FP} \tag{4}$$

Precision: it represents how many of the positive predictions are truly positive. It is calculated as:

$$p = \frac{TP}{FP + TP} \tag{5}$$

Recall: it indicates how many of the positive values were predicted correctly. It is calculated in the following way:

$$r = \frac{TP}{FN + TP} \tag{6}$$

F1-Score: it consists of the harmonic mean between precision and recall. It is expressed by the following formula:

$$F1 = \left(\frac{1}{p} + \frac{1}{r}\right)^{-1} \tag{7}$$

MCC: it is equivalent to the chi-square statistic for a 2 x 2 contingency table. It is calculated as follows:

$$MCC = \frac{TN \times TP - FN \times FP}{\sqrt{(TP + FP)(FP + FN)(TN + FP)(TN + FN)}} \tag{8}$$

Table 1
Comparison of results obtained with different novelty detection algorithms. The table columns report respectively: Type of Algorithm, Accuracy, Precision, Recall, F1 Score, Matthews Correlation Coefficient.

Algorithm	Acc	Precision	Rec	F1	MCC
Isolation Forest	82.90	83.73	92.72	87.32	0.6
SGDSVM	73.93	72.54	**99.94**	83.43	0.3
OneClassSVM	**88.1**	**92.3**	88.3	**89.0**	**0.7**

Table 2
Table of Results Obtained with OneClassSVM. Each row represents a different experiment conducted with a subject. The table columns report the following: ID, Accuracy, Precision, Recall, F1 Score, Matthews Correlation Coefficient, Type of Environment.

Id	Acc	Prec	Rec	F1	MCC	Env
1	97.8	97.2	99.9	98.6	0.9	Out
2	96.6	98.9	97.2	98.0	0.9	Out
3	92.8	92.2	99.5	95.7	0.8	Out
4	74.3	64.8	84.0	73.2	0.5	Out
5	76.6	96.7	69.7	81.0	0.6	Out
6	77.6	92.1	76.5	83.6	0.5	Out
7	90.9	98.6	91.2	94.7	0.6	Out
8	96.8	95.8	99.8	97.8	0.9	In
9	84.9	93.2	84.0	88.3	0.7	In
10	87.8	92.1	86.0	88.9	0.8	In
11	89.2	93.1	89.7	91.4	0.8	In
12	94.3	100	92.2	95.9	0.9	In
13	85.6	84.9	87.2	86.1	0.7	In
Mean	88.1	92.3	89.0	90.2	0.7	

5. Experimental findings

In this section, we present the results of our experimentation.

Our system mainly consists of a module for preprocessing data and a machine learning algorithm that can detect whether or not we are in an anomalous situation at that precise moment. Then, based on control criteria, the primary device sends messages to the worker to warn him of the dangerous condition and the lack of protective device usage. Therefore, we conduct several experiments to verify the correct functioning and check our system's usability.

5.1. Comparison of novelty detection algorithms

In order to choose the best machine learning algorithm to use, we test all three novelty detection algorithms we presented in Section 4.4. We train these algorithms on a dataset representing a single class since the generated model aims to learn to recognize the known class and identify anomalies with respect to that class. For the evaluation, we exploit the datasets we described in Section 4.3. Since the Isolation Forest, the OneClassSGDSVM and the OneClassSVM have several parameters to be set; we perform a parameter tuning approach to find the best way to optimize them according to the nature of the problem. The results obtained from the tests made with optimal parameters are shown in Table 1. The OneClassSGDSVM and the Isolation Forest perform rather well, but among the three algorithms, the OneClassSVM obtains the best results. Considering the results, the machine learning algorithm we chose is the OneClassSVM.

5.2. Machine learning algorithm results

Table 2 illustrates the results we obtain from the OneClassSVM experiments. The table describes for each row the results obtained by the algorithm when trained and tested on a single individual. The final row represents the average of the metrics calculated on the thirteen subjects. The average accuracy of the several experiments is about 88%, and the average precision is about 92%. This positive result indicates that the algorithm correctly recognizes the signal and identifies anomalous events. For example, if we focus on subject #2, they obtain an F-Measure of 98% and an Accuracy of 96.6%. Fig. 9 shows the training dataset collected from the experiment involving subject #2. Fig. 9(a) represents the helmet data, including raw values and the moving average calculated over a 5-second window. Fig. 9(b) shows the data from the shoes. The unprocessed data exhibit peaks and noticeable outliers, but with the moving average processing, they are considerably reduced, and the signal is improved. Fig. 10(a) represents the testing set. The figure shows in detail the result obtained from collecting helmet data and shows RSSI values. The peak in the graph around the second minute and a half represents the moment when the dangerous situation begins, and it corresponds to the movement with which the helmet is removed. In both Figs. 9 and 10(a) the colour intensity represents the value of the Count field, in blue for the helmet and green for the shoes, respectively. Therefore, the more intense the colour of a point, the more detections of that node there were in the time window. In the graph in Fig. 10(a), it can be noticed that there is an area where the colour related to the helmet is very light as it is far away from the subject, and due to the distance, devices make fewer detections. Notably, the shoe average throughout the duration of the experiment remains fairly constant, with few variations. This agrees that the operator constantly wears both shoes throughout the experiment, and the primary device effectively recognizes the difference between near (shoes) and far devices (helmet).

Fig. 10(b) shows the model's results when trained on subject #2. In particular, the figure distinguishes with different colours the points labelled correctly or incorrectly by the model. The different colours represent true negatives in green, true positives in light green, false positives in red and false negatives in orange. In this way, it is possible to observe the points where the algorithm made mistakes and thus better analyse the results obtained. During the peak that happens when the subject removes its helmet, the algorithm classifies the ascent phase incorrectly, as it does not recognize it as abnormal. The classification went very well throughout the entire dangerous situation, with only one small area where the alarm failed around the 3:40 min mark.

5.3. Postprocessing algorithm results

The machine learning algorithm's results identify the situation we are in at any given moment of device use: the velocity at which the devices detect dangerous behaviour is significant. In our use case, we can tolerate the absence of signal for brief moments in which the devices are not worn correctly, for example, when a user momentarily shifts their helmet to drink or other temporary harmless activity. Indeed, if the system reported every little abnormal situation (including small false alarms), users would not be inclined towards using the device as they would be annoyed by the continuous warnings.

For these reasons, in addition to machine learning, we define a postprocessing algorithm that acts as a final control mechanism to detect threats. While the machine learning algorithm detects whether we are in an abnormal situation, the control mechanism calculates if we are in the abnormal situation for a reasonable amount of time. In that case, the control mechanism states there is a danger, and it is necessary to signal the warning to the user.

We have conducted several experiments to determine the ideal threshold of anomalous situation detections to wait for to identify true dangerous situations while avoiding overproducing false positives accurately. We selected possible threshold values from 10 to 80. For each threshold value n, we decide to give an alarm only if the SVM algorithm has classified n consecutive instants as anomalous. The graph in Fig. 7 describes two DET (Detection error tradeoff) curves calculated using the different thresholds. The "overall" curve is generated by combining data from all experiments and calculating metrics as if they belong to a single test. In contrast, the "average" curve is created by calculating each experiment's metrics and then averaging the results. The DET curve is a variation of the ROC curve that uses the False Positive Rate (FPR) and the False Negative Rate (FNR). In this figure, each point is a

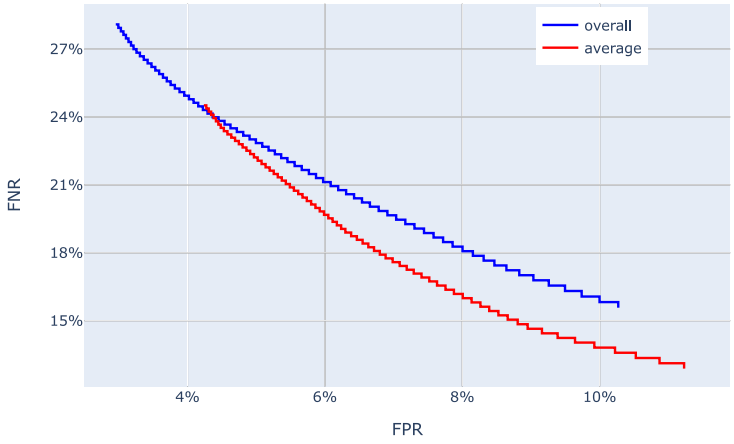


Fig. 7. DET Curve of results plotting the False Negative Rate (FNR) vs. False Positive Rate (FPR). The curve labelled "overall" is constructed by aggregating all the data from all users as if they belong to a single experiment. The curve labelled "average" is obtained by performing calculations on each individual test participant and averaging the results a-posteriori.

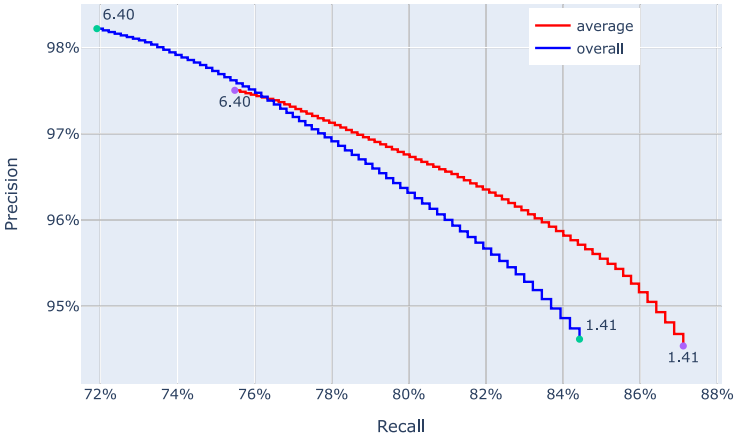


Fig. 8. PR curve representing the relationship between Precision and Recall values using different window sizes. The curve labelled "overall" is constructed by aggregating all the data from all users as if they belong to a single experiment. The curve labelled "average" is obtained by performing calculations on each individual test participant and averaging the results a-posteriori. The green dots are labelled with the delay with which our algorithm sends an alert after an operator has removed a device, expressed in seconds.

result obtained from a particular threshold. When we reach a low FPR, it is clear that we have to suffer a higher FNR. Remarkably, the FPR can achieve extremely low values, and the corresponding FNR is not critically high in respect of our case study.

To identify the proper threshold, it was also necessary to calculate the seconds that, on average, you wait to identify a dangerous situation correctly. Such a period is essential to estimate the effectiveness of our solution because it calculates the time in which there is a danger, and the alarm was not triggered. Fig. 8 shows two PR (Precision–Recall) curves, which represent the performance of our algorithm on the positive class, that is, the anomalous one. In the same way as the DET curve, the two curves are calculated differently to abstract from the characteristic elements of the subjects. In order to show the seconds of delay with which our algorithm sends an alert after an operator has removed a device, the curves show the latency with the shortest window of 10 (1.41 s) and the largest window of 80 (6.40 s). In our approach, we have the ability of fine-tuning the threshold based on the specific use case's requirements, considering the trade-off between false alarms, false negatives and the system latency in detecting critical situations. The size and quality of the dataset has major consequences on the performance of the system, thus the evaluation of the threshold should be made ad-hoc based on the particular use-case. Based on the data collected during our experiments for our use case, we made the decision to set the threshold at 80. With this threshold, we achieve a Precision rate of 98% with a latency of approximately 6 s. This result is aligned with our requirements, as it is critical for us to minimize false positives while maintaining a reasonable response time.

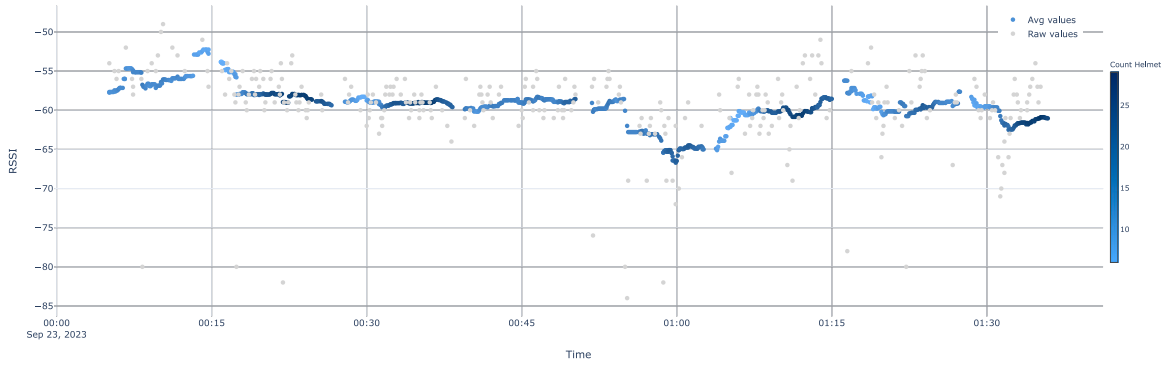
6. Discussion

In this section, we discuss our work. We delve more deeply into its general operation (Section 6.1), analyse how it behaves in different environments (Section 6.2), conduct a usability test (Section 6.3), develop a cost analysis (Section 6.4), investigate privacy and ethics (Section 6.5), compare with related work (Section 6.6) and presents the main limitations (Section 6.7).

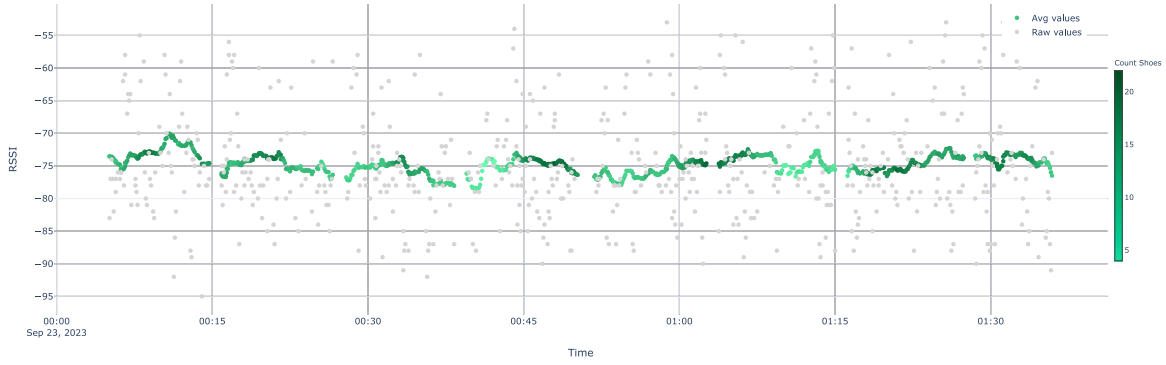
6.1. Usage peculiarities

In order to simplify the demonstration of the effectiveness of the proposed solution and algorithms, we focused on the simplest use case in the previous sections. More specifically, the use case involves the regular use of the devices by an operator wearing a helmet and safety shoes and the subsequent removal of the helmet, resulting in the activation of the alarm. However, more varied situations can occur, and the current section explores how the system would behave in such cases.

Work break management. Since the current system monitors the use of PPE, if the operator accidentally removes a device, then the alarm sounds. However, there may be cases where removing PPE is not a



(a) RSSI values of the Helmet



(b) RSSI values of the Shoes

Fig. 9. Scatter Plot Representing Data for Subject #2 collected within the experiments and stored in the dataset attached to this paper. Both the subfigures represent the time series of the measured RSSI values against the acquisition time. The subfigure (a) depicts data collected by the secondary node mounted on the subject's helmet, while the subfigure (b) illustrates data collected by secondary nodes attached to the subject's shoes, and in particular the averaged values of right and left shoes.

hazard. An example of such a case is a work break. To distinguish these cases, we designed a specific programmable pushbutton on our prototype device, which can be configured to accept both short and long presses. In the first case, the device resets the alarm state, while in the second case, the device temporarily deactivates to allow the worker to take a break. This feature not only enhances the safety of our system but also promotes worker well-being by giving them the flexibility to pause their monitoring when needed.

Noise protection equipment. Our device includes an OLED display and an acoustic buzzer. Therefore, an operator is capable of receiving the alarm notification unless they have limitations in hearing or vision. This implementation aligns well with our specific use case. In situations where other Personal Protective Equipment (PPE) might limit a worker's senses, it may be prudent to consider additional alerting mechanisms such as vibrators or flashing lights. These potential enhancements could be part of future work proposals.

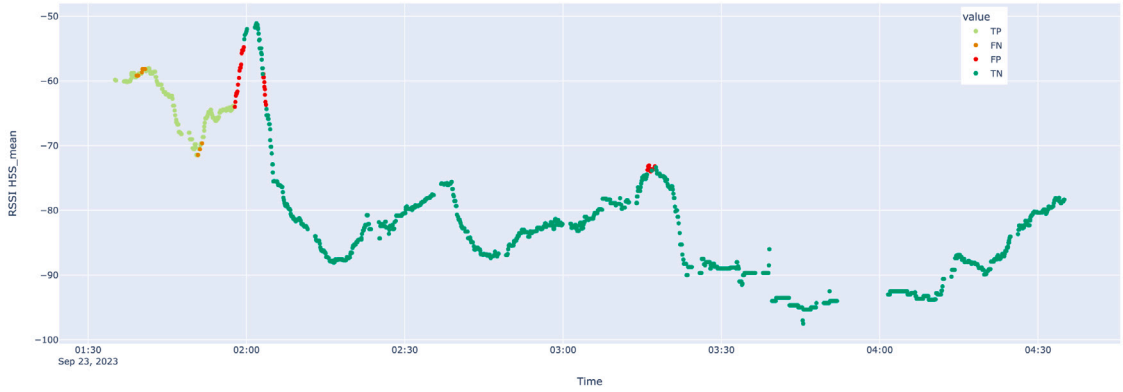
Potential fault cases. It is crucial to take into account some solutions to address edge use cases that may negatively impact the system's robustness. Generally, both primary and secondary devices provide an intuitive visual signalling to the operator through the status LED, which turns red whenever the device detects an issue. Since our architecture is composed of components of different types, our analysis of potential failures must consider and distinguish different cases, and we analyse them below. It is possible to identify three potential fault cases, and for each of them, we define what can happen and how the problem is mitigated. Secondary node fault: Since secondary nodes work with a broadcast strategy, only the workers can detect their faults. At the beginning of each work shift, each worker has to execute a functional check to evaluate the proper functioning of the devices. For example, during the training phase, the entire functioning of the system can be checked in order to prevent the use of malfunctioning devices. Moreover, the primary device displays a message on the LCD to indicate that it is receiving messages from the secondary devices, thus providing a visual signal that the device is functioning correctly. In addition, it is possible to add a LED status on the secondary devices that alerts when they send messages in broadcast correctly to provide another visual signal of failures. Primary node fault: Primary node faults can be detected at the worksite's central unit level. The central unit is responsible for collecting the messages from each worker's primary device and sending them to the cloud. In addition, it is possible to implement a continuous exchange of keep-alive signals that can ensure that the connection between the primary device and the central unit has not been interrupted. When the central unit does not receive this signal from a primary device in a certain amount of time, a proactive alert can be triggered and the worksite supervisor will be informed of the malfunctioning device. Central unit fault: Thanks to the exchange of keep-alive signals, the primary devices can detect central unit failures as they no longer receive such signals. The primary devices can report the problem to the worker and start internal logging of anomalies. The monitoring data may be recovered from the primary device or can be sent to the central unit after the communication is restored. Finally, operators can cancel the alarm by pressing the dedicated button to maintain control in cases of false alarms, offering a streamlined and user-friendly approach to managing potential false positives.

6.2. Complex environments

As shown in the previous section, we tested the system both in an outdoor (and interference-free) environment and an indoor (and noisy) environment. This section investigates how the system may behave in other environments, what possible challenges may emerge, and how they can be addressed.

Large workplaces and scalability. Our proposed approach has good scalability characteristics, thanks to its foundation on an inherently scalable IoT architecture based on Fog computing (Dastjerdi, Gupta,

(a) Average values of the helmet and the shoes



(b) Results obtained by the SVM trained and tested on subject #2.

Fig. 10. Scatter Plot Representing Data for Subject #2 collected within the experiments and stored in the dataset attached to this paper. Both the subfigures represent the averaged time series of the measured RSSI values against the acquisition time. The subfigure (a) depicts averaged data collected by the secondary nodes mounted on the subject's helmet and shoes versus the acquisition time, while the subfigure (b) illustrates the results of executing the SVM model versus the same time scale. The colour scale allows understanding the data density and the performance of the algorithm.

Calheiros, Ghosh, & Buyya, 2016). Our architecture enables the reduction of data transfer to the cloud, optimizing the performance and latencies of IoT solutions. Consequently, adding an arbitrary number of devices and workplaces to the monitoring platform becomes possible, and the system will scale accordingly. This feature has good sustainability in that adding more workers or workplaces does not require any modification to the cloud system, as we can also discuss in Section 6.4. From a workplace perspective, unlike the architectures examined in the literature review, our solution does not require the installation of cameras or dedicated devices. It only necessitates ensuring solid WiFi signal coverage throughout the construction site, which needs proper distribution of routers on-site.

Small and noisy workplaces. When assessing the applicability of our solution within specific industries, it is crucial to consider whether the environment permits the unimpeded propagation of BLE and WiFi signals to ensure seamless device communication. In some specific scenarios, such as underground mining, where the advancing excavation process may challenge signal propagation, robust electromagnetic interference can disrupt BLE communication and compromise the body area network viability. Among the possible solutions, we suggest implementing mesh-based networks with synchronous flooding or using resilient radio technologies such as narrowband IoT to maintain reliable communication. Considerations must also be given to the robustness of the AI model in the face of external disruptions. We conducted tests under varying conditions, encompassing both indoor and outdoor settings, and observed successful performance. However, it is important to acknowledge that unique environmental circumstances may necessitate retraining of the AI models.

6.3. System usability

While in the first outdoor test, we worked on validating the idea and algorithms, starting with the second test we gave more attention to the system's usability. For this reason, we subjected all participants in the indoor testing phase to a usability test, the System Usability Scale (SUS) (Brooke, 1996). The test consists of ten questions answered by a grade from 1 to 5 based on how much each participant agrees or disagrees with the proposed statement. The statements are the following.

- I think that I would like to use this system frequently.
- I found the system unnecessarily complex.
- I thought the system was easy to use.
- I think that I would need the support of a technical person to be able to use this system.
- I found the various functions in this system were well integrated.
- I thought there was too much inconsistency in this system.
- I would imagine that most people would learn to use this system very quickly.
- I found the system very cumbersome to use.
- I felt very confident using the system.
- I needed to learn a lot of things before I could get going with this system.

The SUS provides formulas by which the votes entered by users are converted into a score from 0 to 100. The average user rating was 86.67, a very good score. We highlight that the system we developed is a prototype for which, in this paper, we focus more on validating the scientific part related to the algorithms. Moreover, the system can be further miniaturized to improve its usability even more.

6.4. Cost analysis

To tackle the problem of estimating the costs of our solution, we provide a contribution by estimating the cost of a setup for a single

Table 3
Cost analysis based on the bill of materials of the proposed prototype solution.

			Price (EUR)		
Architecture layer	Component	Cost type	1 worker 1 worksite	5 workers 1 worksite	10 workers 2 worksites
Sensors and Edge Layers	*TinyS3*	One-off	100	5000	1000
	OLED display	One-off	20	100	200
	Buzzer	One-off	3	15	30
	Push Button	One-off	3	15	30
	Battery	One-off	65	325	650
	Housing and cables	One-off	9	45	90
Fog Layer	Wireless router	One-off	100	100	200
	Central Unit	One-off	80	80	160
Cloud Layer	Cloud Infrastructure	Monthly	100	100	100
	Deployment cost	One-off	480	1280	2560
	Maintenance costs	Monthly	100	100	100

body area network, and then extend the evaluation to a workplace characterized by a particular number of workers. Each worker needs three secondary devices and a primary device. The worksite needs to be provided with enough WiFi routers to cover the area and a central unit to collect data from the primary devices. Also, in a real-world application, a cloud service must be up and running to serve the cloud-based platform.

Our devices are currently in the prototype stage, and it is important to note that the associated costs are distinct from those of large-scale production. The costs of our prototype solution is represented in Table 3. The expenses related to engineering and manufacturing the devices at scale, without relying on development boards and commercial products, would inherently differ significantly. Given that the firmware is released open-source, the price threshold that we can identify as a lower bound for each device is EUR 1.70, which is the price of an ESP32-S3 System-on-Chip. Also, the environmental conditions of the worksite may require to utilization of particular components, such as electronic devices with resistance to high temperature or strong vibrations, or particularly effective wireless access points, which may increase the price of devices.

To evaluate the benefit of implementing such a solution with respect to its cost, the employer has to consider performing an economic evaluation of investments for workplace safety, such as the one introduced by the scientific paper (Bianchini, Pellegrini, Peta, Saccani, et al., 2014). According to the latter paper, the average cost of a single accident in the country of Italy is about EUR 27000, much higher than the cost of investing in our solution. However, each employer has to conduct its own evaluation based on the return on the investment, also considering the social impact of having a safer work environment.

6.5. Privacy and ethical considerations

Regarding the ethics in work monitoring, it is necessary to inform operators fully about the ongoing monitoring, enabling them to receive training on interacting correctly with the system. Also, ensuring that the system cannot be used for purposes other than monitoring the devices is crucial.

We have designed our system to minimize the impact on operators' privacy. Indeed, the data collected during monitoring measures the intensity of the communication signal between the devices worn. No photographic data, video or information on the movements performed by the worker is collected. Since the type of data we handle is very generic and abstract concerning the user's activities, the operator is not controlled in their movements but only by the correct use of any device worn. We highlight that this factor is one of the strengths of our approach, allowing us to differentiate ourselves from all other work that instead saves explicit data on operator behaviour (such as all the "device-free" works that, although they do not use IoT devices but only use cameras, have a significant impact on privacy because they are constantly filming operators).

In addition, we designed the system architecture so that the signal from the operator's devices is not saved outside the workplace (e.g., in a cloud platform). The IoT devices compute the signal and immediately remove it to process subsequent signals. Indeed, this signal strength information is collected internally in the primary device (the belt), which, after processing it and determining whether the user is using the devices, only outputs messages indicating whether the PPEs are worn correctly. The system only sends this intensity data towards the fog layer during training, but the operator must be aware of collecting this data at this stage.

The ethical framework within which the system operates is defined by a strict focus on device usage verification without data collection from the user, except for the signal strength used in the model's training. Our architectural choice allows us to protect the operator's privacy and simultaneously reduce the resource consumption of IoT devices (energy, bandwidth) with numerous benefits in terms of privacy and usability.

6.6. Comparison with related work

The scientific literature on PPE monitoring encompasses various approaches and techniques. In this section, we will examine some of these methods, as outlined in Table 4, and propose a qualitative comparison using the metrics detailed in Section 3.1. Additionally, we have introduced two additional criteria for categorization: (i) the methodology of analysis and (ii) the type of instrumentation employed. With the first criterion, we distinguish between works that implement analysis as a one-shot solution (e.g., by introducing an instrumented gate) and those that perform continuous, always-on analysis. With the second criterion, we categorize works based on the type of instrumentation used, whether it is applied to the environment, directly on individuals, or on the instruments they use and wear.

Each metric is assessed in the table by assigning points to the works using empty, half-full, or full circles. For the efficacy metric, we evaluate the presence of any conditions that may introduce noise in the values and, if such conditions exist, the system's ability to mitigate their effects. Regarding the usability metric, we assess how seamlessly the user can adapt to using the proposed solution, assigning the highest score to solutions that are transparent to the user and the lowest score to those that may impede the user's movements. For the portability metric, we evaluate how easily the proposed solution can be adapted to new working contexts. The scalability metric assesses the complexity of implementing the proposed solution and its suitability for accommodating a large number of users. Traceability and privacy preservation are binary metrics that evaluate the system's capability to track transactions for future audits and maintain user privacy.

Earlier works introduced IoT solutions for monitoring PPEs using a Body Area Network (BAN) where devices communicate via RFID technology or, in some cases, cables. For instance, Barro-Torres et al. (2012)

Table 4
Qualitative comparison of related works. Abbreviations list: Instrumentation (Inst.), Computer Vision (CV), Personal (per.), Environmental (env.), Accelerometers (Acc.)

Work	Year	Method	Inst.	Efficacy	Usability	Portability	Scalability	Traceability	Privacy	Technology
Kelm et al. (2013)	2013	one-shot	per.	●●	●●	●●	●●	●	●	RFID
Hayward et al. (2022)	2022	one-shot	per.	●●	●●	●●	●●	●	●	RFID
Barro-Torres et al. (2012)	2012	always-on	env.	●◐	◐○	◐○	●◐	●	●	RFID
Sole et al. (2013)	2013	always-on	env.	●◐	◐○	◐○	●◐	○	●	RFID
Gu et al. (2019)	2019	always-on	env.	●◐	●●	◐○	●●	●	○	CV
Delhi et al. (2020)	2020	always-on	env.	●◐	●●	◐○	●●	○	○	CV
Wu et al. (2019)	2020	always-on	env.	●◐	●●	◐○	●●	●	○	CV
Xiong et al. (2022)	2022	always-on	env.	●◐	●●	◐○	●●	●	○	CV
Kim et al. (2018)	2018	always-on	per.	●◐	●◐	●○	●●	●	●	Acc.
Yang et al. (2020)	2020	always-on	per.	●●	●◐	●●	◐○	●	●	Ad-hoc
Abbasianjahromi and Sohrab Ghazvini (2021)	2022	always-on	per.	●●	◐○	●◐	●○	●	●	Magnets
This work		always-on	per.	●◐	●◐	●●	●●	●	●	BLE RSSI

developed a system that necessitates each worker to wear a BAN, with RFID sensors embedded in the PPEs. The BAN of sensors detects each PPE at specific body points, ensuring correct device positioning in real time. However, this system requires cables connecting BAN devices, which can significantly impact worker mobility, as they must wear a network of wires connecting their shoes, vests, and helmets. In contrast, the approach we propose ensures unrestricted operator movement as communication between nodes occurs via BLE, eliminating the need for cables.

Authors of Sole et al. (2013) suggest the usage of an architecture based on two networks. The first is a BAN, where each PPE contains a device integrating an RFID tag, while other devices include sensor units. The second network consists of fixed nodes at strategic control points in the working environment. Each node uses stationary RFID readers to detect tags within a one-metre range, transmitting status tags to a data processing system. However, the setup required for the workplace to support RFID tag detection leads to increased time and costs for PPE monitoring, limiting its efficiency in larger workplaces.

Kelm et al. (2013) and, more recently, Hayward et al. (2022), propose a system utilizing a smart portal equipped with antennas at workplace entrances. Workers are provided with RFID tags associated with their PPE, and the portal verifies proper usage as workers pass through. However, this approach only verifies compliance at the beginning and at the end of a work activity, lacking continuous monitoring during tasks.

More recent developments employ real-time image acquisition through cameras to identify PPE usage and assess whether they are correctly worn. Specifically, this approach involves installing cameras in the workplace, continuously filming workers, and sending images to a remote system that employs computer vision algorithms to identify workers not wearing PPEs. For example, Gu et al. (2019) employs an improved Faster RCNN to determine if workers are wearing safety helmets, achieving improved detection accuracy, especially in low-light conditions and with occluded images. Delhi et al. (2020) applies convolutional neural networks through transfer learning to a simplified version of the YOLOv3 deep learning network for detecting safety helmets and safety vests on construction sites. An alarm is triggered when the model detects the absence of PPEs. Xiong et al. (2022) embeds the YOLOv3 algorithm into IoT devices and employs coordinated recognition to obtain results from multiple angles. Similarly, Wu et al. (2019) proposes a CNN-based method using cameras for real-time monitoring of helmet usage. However, these computer vision approaches differ from our approach as they share the limitation of requiring prior workplace setup (installation of cameras), increasing both time and costs. Additionally, they are susceptible to occlusions and adverse weather conditions.

Other works suggest a BAN of devices communicating through wireless technologies like Wi-Fi and BLE, which aligns closely with our approach using a BAN of BLE devices. For instance, Abbasianjahromi and Sohrab Ghazvini (2021) applies wearable devices with magnetic sensors to each PPE. These devices transmit information to a central device located in the operator's jacket, which in turn relays operator status to a smartphone application via Wi-Fi. Yang et al. (2020) develops an automated control system for coupling PPE with tools, alerting safety officers and triggering alarms when individuals are not wearing the required PPE while using tools. This system equips both tools and PPE with sensors, with tools receiving information via Wi-Fi to verify proper usage.

Kim et al. (2018) focuses on safety-helmet detection using a three-axis accelerometer sensor, achieving a high level of accuracy in detecting proper use, improper use, and non-use of protective headgear. Additionally, Booranawong et al. (2018) presents a device-free system for tracking and detecting humans indoors using RSSI, successfully detecting human movements in various experiments.

Finally, some recent works, such as Campero-Jurado et al. (2020), introduce smart helmets equipped with instrumentation for monitoring environmental conditions and alerting workers to hazardous situations, such as the presence of harmful gases. Although these works employ IoT for workplace safety, they differ from our approach as they do not primarily focus on verifying PPE or helmet usage but rather concentrate on monitoring environmental parameters. In a similar way, Rescio et al. (2023) proposes a wearable system to monitor workers' stress levels, primarily concerned with monitoring workers' health rather than verifying PPE use.

In the context of works categorized as active monitoring and personal instrumentation, our approach distinguishes itself by its adaptability to different environments and its capacity to handle noisy data. Furthermore, it stands out for its excellent scalability and straightforward implementation, as it does not require specific sensors or a complex remote data analysis system. The remote system remains streamlined while maintaining the ability to trace system operations and safeguard user privacy.

6.7. Limitations

The effectiveness of our system relies on workers using PPE equipped with BLE-enabled IoT devices. Compatibility issues may arise when integrating these devices into existing PPE or ensuring all workers have access to them. Although our solution demonstrates resilience to environmental factors, extreme conditions, such as dense electromagnetic interference or severe weather, could affect the system's performance. The implementation of real-time monitoring raises

privacy considerations. Balancing safety with worker privacy rights requires careful planning and ethical considerations.

Workers' acceptance and adaptation to continuous monitoring may vary. Some individuals may be resistant to the idea of being constantly monitored, necessitating strategies for user education and engagement. Scaling the system to larger workplaces or industrial settings may present challenges in terms of network management and data processing, which should be carefully addressed. The accuracy of our anomaly detection algorithm may be influenced by factors not explored in this study. Further research is needed to fine-tune the system's sensitivity. Ongoing ethical considerations surround the monitoring of workers, requiring a well-defined ethical framework and potential regulatory compliance. These limitations should be taken into account when considering the implementation of our proposed solution and provide directions for future research and development efforts.

7. Conclusions and future work

Our work aims to address the research questions introduced in Section 1, showing that the answer for both questions is yes, (RQ1) it is possible to use the RSSI signal and (RQ2) it is possible to build a simple and adaptable learning system for different application scenarios that can identify anomalies in the use of common personal protective equipment.

First, we have defined the requirements for a system to overcome current limitations and designed an architecture to reflect the identified requirements. Then, we exploited commercial electronic devices provided with Bluetooth Low Energy (BLE) technology to build IoT devices able to communicate within the OAN to detect if the worker is properly wearing its PPEs. We developed and tested different machine learning algorithms to be embedded within the primary device, the OAN's central node. The algorithm in the primary device processes the Receive Signal Strength Indicator (RSSI) signals from the secondary devices to detect whether the PPEs are used correctly by identifying an RSSI signature. ML allows the detection of the correct wearing of the PPE and makes the approach robust concerning environmental and operator conditions.

We evaluated the effectiveness of our solution by detecting the correct position of a helmet. We show that our algorithm achieves 88% accuracy, which we further improve by playing with the trade-off between false alarms and detection delay. We have shown that overall, the system reports the abnormal helmet removal event within a little more than 6 s of the event.

Experimental tests support the feasibility of BLE technology as a low-cost and low-power monitoring solution for PPE usage. The resulting devices to be mounted on PPEs are economically accessible and easy to set up. They are also non-invasive in not interfering with the workers' common movements and activities.

Future works may include extensions like designing similar systems applied to different PPEs; testing our current approach to entirely different use cases; extending the system to support near-miss detection; and combining information from our sensors with other data to create an increasingly refined digital twin of the workplace (Lugaresi, Gangemi, Gazzoni, & Matta, 2023); designing the presented devices for harsh environments; exploring appropriate signalling mechanisms when workers are equipped with PPEs that impair their ability to see, hear, or sense their surroundings effectively. Moreover, in future work, we would like to explore the application of our architecture in other use cases related to occupational safety and other domains. For instance, control the distance between workers and hazardous machinery to ensure that workers do not get closer than necessary and thus prevent potential hazards. Another possible use case is to expand the system by adding environmental sensors to monitor the environment surrounding the worker and ensure that the workplace is in the best condition.

CRediT authorship contribution statement

Alessia Pisu: Conceptualization, Investigation, Resources, Software, Data curation, Validation, Visualization, Writing – original draft, Writing – review & editing. **Nicola Elia:** Conceptualization, Software, Data curation, Validation, Visualization, Writing – original draft, Writing – review & editing. **Livio Pompianu:** Conceptualization, Investigation, Resources, Methodology, Visualization, Writing – original draft, Writing – review & editing, Supervision. **Francesco Barchi:** Conceptualization, Methodology, Visualization, Writing – original draft, Writing – review & editing. **Andrea Acquaviva:** Conceptualization, Writing – review & editing, Project administration. **Salvatore Carta:** Conceptualization, Writing – review & editing, Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

We have released a GitHub repository containing all data and code.

Acknowledgments

This work is partially supported by Aut. Reg. of Sardinia Programma Regionale di Sviluppo 2020-2024, project "Security for Worker". Alessia Pisu and Livio Pompianu acknowledge MUR and EU-FSE for financial support of the PON Research and Innovation 2014-2020 (respectively D.M. 1061/2021 and D.M 1062/2021 programs). Nicola Elia acknowledges support from TIM S.p.A. through the PhD scholarship. The authors thank all participants for their willingness and support to the experimental phase. The authors also thank Sebastian Podda for his insightful comments on a preliminary version of this paper.

References

Firmware and dataset repository, https://anonymous.4open.science/r/aiot-based-ppe-monitoring-C6A9.

ESP32-S3 datasheet. (2023). https://www.espressif.com/sites/default/files/documentation/esp32-s3_datasheet_en.pdf, [Online; accessed 2023/02/16].

Micropython project repository. (2023). https://github.com/micropython/micropython, [Online; accessed 2023/02/16].

Abbasianjahromi, H., & Sohrab Ghazvini, E. (2021). Developing a wearable device based on IoT to monitor the use of personal protective equipment in construction projects. *Iranian Journal of Science and Technology, Transactions of Civil Engineering*, 1–13.

Ammad, S., Alaloul, W. S., Saad, S., & Qureshi, A. H. (2021). Personal protective equipment (PPE) usage in construction projects: A scientometric approach. *Journal of Building Engineering*, *35*, Article 102086.

Asadzadeh, A., Arashpour, M., Li, H., Ngo, T., Bab-Hadiashar, A., & Rashidi, A. (2020). Sensor-based safety management. *Automation in Construction*, *113*, Article 103128. http://dx.doi.org/10.1016/j.autcon.2020.103128, URL https://www.sciencedirect.com/science/article/pii/S0926580519305679.

Barro-Torres, S., Fernández-Caramés, T. M., Pérez-Iglesias, H. J., & Escudero, C. J. (2012). Real-time personal protective equipment monitoring system. *Computer Communications*, *36*(1), 42–50.

Bianchini, A., Pellegrini, M., Peta, D., Saccani, C., et al. (2014). Economic evaluation of investments for workplace safety. *Chemical Engineering*, *36*, 49–54.

Booranawong, A., Jindapetch, N., & Saito, H. (2018). A system for detection and tracking of human movements using RSSI signals. *IEEE Sensors Journal*, *18*(6), 2531–2544. http://dx.doi.org/10.1109/jsen.2018.2795747.

Brooke, J. (1996). Sus: A "quick and dirty'usability. *Usability Evaluation in Industry*, *189*(3), 189–194.

Campero-Jurado, I., Márquez-Sánchez, S., Quintanar-Gómez, J., Rodríguez, S., & Corchado, J. M. (2020). Smart helmet 5.0 for industrial internet of things using artificial intelligence. *Sensors*, *20*(21), 6241.

Dastjerdi, A. V., Gupta, H., Calheiros, R. N., Ghosh, S. K., & Buyya, R. (2016). Fog computing: Principles, architectures, and applications. In *Internet of things* (pp. 61–75). Elsevier.

Davidescu, A. A., et al. (2020). Work flexibility, job satisfaction, and job performance among Romanian employees–implications for sustainable human resource management. *Sustainability*, *12*(15), 6086. http://dx.doi.org/10.3390/su12156086.

Delhi, V. S. K., Sankarlal, R., & Thomas, A. (2020). Detection of personal protective equipment (PPE) compliance on construction site using computer vision based deep learning techniques. *Frontiers in Built Environment*, *6*, http://dx.doi.org/10.3389/fbuil.2020.00136, URL https://www.frontiersin.org/articles/10.3389/fbuil.2020.00136.

Eurostat (2022). Eurostat accident at work statistics. Accessed: 2022-09-13.

Greubel, J., et al. (2016). Higher risks when working unusual times? A cross-validation of the effects on safety, health, and work–life balance. *International Archives of Occupational and Environmental Health*, *89*(8), http://dx.doi.org/10.1007/s00420-016-1157-z.

Gu, Y., Xu, S., Wang, Y., & Shi, L. (2019). An advanced deep learning approach for safety helmet wearing detection. In *2019 International conference on internet of things (IThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)* (pp. 669–674). http://dx.doi.org/10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00128.

Haar, J. M., et al. (2014). Outcomes of work-life balance on job satisfaction, life satisfaction and mental health: A study across seven cultures. *Journal of Vocational Behavior*, *85*(3), 361–373. http://dx.doi.org/10.1016/j.jvb.2014.08.010.

Hayward, S., van Lopik, K., & West, A. (2022). A holistic approach to health and safety monitoring: Framework and technology perspective. *Internet of Things*, *20*, Article 100606.

Heydon, R., & Hunn, N. (2012). Bluetooth low energy. *CSR Presentation, Bluetooth SIG*, https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx.

Ji, T., Li, W., Zhu, X., & Liu, M. (2022). Survey on indoor fingerprint localization for BLE. In *2022 IEEE 6th information technology and mechatronics engineering conference (ITOEC), Vol. 6* (pp. 129–134). Ieee.

Kelm, A., Laußat, L., Meins-Becker, A., Platz, D., Khazaee, M. J., Costin, A. M., et al. (2013). Mobile passive radio frequency identification (RFID) portal for automated and rapid control of personal protective equipment (PPE) on construction sites. *Automation in Construction*, *36*, 38–52.

Kim, S. H., Wang, C., Min, S. D., & Lee, S. H. (2018). Safety helmet wearing management system for construction workers using three-axis accelerometer sensor. *Applied Sciences*, *8*(12), 2400.

Kumar, P., Reddy, L., & Varma, S. (2009). Distance measurement and error estimation scheme for RSSI based localization in wireless sensor networks. In *2009 Fifth international conference on wireless communication and sensor networks* (pp. 1–4). Ieee.

Li, H., Li, X., Luo, X., & Siebert, J. (2017). Investigation of the causality patterns of non-helmet use behavior of construction workers. *Automation in Construction*, *80*, 95–103.

Lugaresi, G., Gangemi, S., Gazzoni, G., & Matta, A. (2023). Online validation of digital twins for manufacturing systems. *Computers in Industry*, *150*, Article 103942.

Parmar, M., Kelly, P., & Berry, D. (2022). Effects of body occlusion on bluetooth low energy RSSI in identifying close proximity of pedestrians in outdoor environments. In *2022 IEEE international smart cities conference* (pp. 1–7). Ieee.

Pascacio, P., Casteleyn, S., & Torres-Sospedra, J. (2021). Smartphone distance estimation based on RSSI-fuzzy classification approach. In *2021 International conference on localization and GNSS* (pp. 1–6). Ieee.

Pilati, F., & Sbaragli, A. (2023). Learning human-process interaction in manual manufacturing job shops through indoor positioning systems. *Computers in Industry*, *151*, Article 103984.

Pu, C.-C., & Chung, W.-Y. (2008). Mitigation of multipath fading effects to improve indoor RSSI performance. *IEEE Sensors Journal*, *8*(11), 1884–1886.

Rescio, G., Manni, A., Caroppo, A., Ciccarelli, M., Papetti, A., & Leone, A. (2023). Ambient and wearable system for workers' stress evaluation. *Computers in Industry*, *148*, Article 103905.

Singh, N., Choe, S., & Punmiya, R. (2021). Machine learning based indoor localization using wi-fi RSSI fingerprints: An overview. *IEEE Access*, *9*, 127150–127174.

Sole, M., Musu, C., Boi, F., Giusto, D., & Popescu, V. (2013). RFID sensor network for workplace safety management. In *2013 IEEE 18th conference on emerging technologies & factory automation* (pp. 1–4). http://dx.doi.org/10.1109/etfa.2013.6648157.

Thaljaoui, A., Val, T., Nasri, N., & Brulin, D. (2015). BLE localization using RSSI measurements and iringla. In *2015 IEEE international conference on industrial technology* (pp. 2178–2183). http://dx.doi.org/10.1109/icit.2015.7125418.

Tutak, M., et al. (2022). Evaluating differences in the level of working conditions between the european union member states using topsis and k-means methods. *Decision Making Applications in Management and Engineering*, *5*(2), http://dx.doi.org/10.31181/dmame0305102022t, 2620–0104.

Wang, Y., Yang, X., Zhao, Y., Liu, Y., & Cuthbert, L. (2013). Bluetooth positioning using RSSI and triangulation methods. In *2013 IEEE 10th consumer communications and networking conference* (pp. 837–842). http://dx.doi.org/10.1109/ccnc.2013.6488558.

Wong, T. K. M., Man, S. S., & Chan, A. H. S. (2020). Critical factors for the use or non-use of personal protective equipment amongst construction workers. *Safety Science*, *126*, Article 104663.

Wu, J., Cai, N., Chen, W., Wang, H., & Wang, G. (2019). Automatic detection of hardhats worn by construction personnel: A deep learning approach and benchmark dataset. *Automation in Construction*, *106*, Article 102894. http://dx.doi.org/10.1016/j.autcon.2019.102894, URL https://www.sciencedirect.com/science/article/pii/S092658051930264X.

Wu, R.-H., Lee, Y.-H., Tseng, H.-W., Jan, Y.-G., & Chuang, M.-H. (2008). Study of characteristics of RSSI signal. In *2008 IEEE international conference on industrial technology* (pp. 1–3). http://dx.doi.org/10.1109/icit.2008.4608603.

Xiong, F., Xu, C., Ren, W., Zheng, R., Gong, P., & Ren, Y. (2022). A blockchain-based edge collaborative detection scheme for construction internet of things. *Automation in Construction*, *134*, Article 104066. http://dx.doi.org/10.1016/j.autcon.2021.104066.

Yang, X., Yu, Y., Shirowzhan, S., sepasgozar, S., & Li, H. (2020). Automated PPE-tool pair check system for construction safety using smart IoT. *Journal of Building Engineering*, *32*, Article 101721. http://dx.doi.org/10.1016/j.jobe.2020.101721, URL https://www.sciencedirect.com/science/article/pii/S2352710220333544.

Yilmaz, G., Salter, L., McFarlane, D., & Schönfuß, B. (2023). Low-cost (shoestring) digital solution areas for enabling digitalisation in construction SMEs. *Computers in Industry*, *150*, Article 103941.