International Journal on Interactive Design and Manufacturing (IJIDeM) (2023) 17:421–433
https://doi.org/10.1007/s12008-022-01035-4

ORIGINAL PAPER

Smart retrofitting for human factors: a face recognition-based system proposal

Andrea Generosi[1] · Thomas Agostinelli[1] · Maura Mengoni[1]

Received: 7 March 2022 / Accepted: 10 August 2022 / Published online: 18 September 2022

Abstract

Industry nowadays must deal with the so called "fourth industrial revolution", i.e. Industry 4.0. This revolution is based on the introduction of new paradigms in the manufacturing industry such as flexibility, efficiency, safety, digitization, big data analysis and interconnection. However, human factors' integration is usually not considered, although included as one of the paradigms. Some of these human factors' most overlooked aspects are the customization of the worker's user experience and on-board safety. Moreover, the issue of integrating state of the art technologies on legacy machines is also of utmost importance, as it can make a considerable difference on the economic and environmental aspects of their management, by extending the machine's life cycle. In response to this issue, the Retrofitting paradigm, the addition of new technologies to legacy machines, has been considered. In this paper we propose a novel modular system architecture for secure authentication and worker's log-in/log-out traceability based on face recognition and on state-of-the-art Deep Learning and Computer Vision techniques, as Convolutional Neural Networks. Starting from the proposed architecture, we developed and tested a device designed to retrofit legacy machines with such capabilities, keeping particular attention to the interface usability in the design phase, little considered in retrofitting applications along with other Human Factors, despite being one of the pillars of Industry 4.0. This research work's results showed a dramatic improvement regarding machines on-board access safety.

Keywords Smart retrofitting · Industry 4.0 · Industrial Internet of Things · Face recognition · Safety · Usability

1 Introduction

Today industry is witnessing, in a process that has been going on for many years, the phenomenon of Industry 4.0. This phenomenon, of such importance as to be considered the fourth industrial revolution [1], has introduced new paradigms within industrial production, based on concepts such as flexibility, efficiency, safety, digitization, big data analysis and interconnection [2]. In this context, the research focus is on the application of Industry 4.0 paradigms to the design and manufacture of a new generation of industrial machinery. Companies are moving toward Internet-connected machines (Industrial Internet of Things, namely IIoT [3]) enabling mutual communication even when located in different production plants. Machines are equipped with a set of sensors monitoring different parameters such as vibration, noise, temperature, energy consumption, useful to predict machine failures thanks to Machine Learning algorithms [4, 5] Another challenging issue leading the transition from Industry 4.0 to 5.0 is the paradigm of personalized human–machine interaction (HMI) [6], that implies exploiting user's biometric data to customize machine operation and improve on-board safety. Biometric recognition can be based either on face, iris, voice, finger or palm recognition. It could become a tool to allow safer access to machine functions only to authorized people, in a safer and more reliable way than with traditional passwords and alphanumeric PINs. The importance of biometric recognition in machine development emerges from both the analysis of literature on current HMI

Andrea Generosi, Thomas Agostinelli and Maura Mengoni contributed equally to this work.

✉ Maura Mengoni
m.mengoni@univpm.it

Andrea Generosi
a.generosi@univpm.it

Thomas Agostinelli
t.agostinelli@pm.univpm.it

[1] Department of Industrial Engineering and Mathematical Sciences, Università Politecnica delle Marche, Via Brecce Bianche, 12, 60131 Ancona, AN, Italy

for IIoT machines and practice in manufacturing. This analysis leads to the formulation of two problems where biometric recognition can be a solution:

- *Personnel authentication* access to the highest level of system information is allowed only to a trained maintenance technician or to the administrator of the production plant. Some of this information, of a purely diagnostic nature, is not needed by the operator during normal operations. Moreover, not all the parameters of a machine can be changed during the machine's operations or, worse, by an operator without a full knowledge of how the machines reacts to those changes. To intervene on the parameters there is a need for careful planning upstream of the production, as well as the necessary knowledge to be able to predict the effect of the changes on the result. Unfortunately, as already mentioned, access is often granted only through an alphanumeric password that quickly becomes public knowledge, being shared even with unauthorized personnel.
- *Log files usability* another problem that arises from the use of legacy machinery is tracking the operations performed by reading the log files, especially about user's log-in and log-outs, procedures that are usually not reliable (sometimes being the password the machine's serial number and so not user-related). Thanks to the user's secure identification obtained with biometric data, the information on the identity of those who have carried out the operations becomes trustworthy. This authentication method also guarantees lower access times and does not imply any slowdown in operations: authentication can be done for every user's movement between different machines. In this way a history of each activity is recorded and associated with the single user. Moreover, native log files are often not easily readable, given their interpretation is left to technical staff or, more frequently, to employees of the company that produced the machine [7]. However, due to the smart nature of next-generation machines, a new log file can be created, parallel to the native one. This secondary log file can be tailored to the needs of the business, without the need to contact the company that originally manufactured the machine (or PLC) to make changes to the native log file, an activity often provided for a fee. Finally, thanks to IIoT devices, these files can be accessed remotely and in real time.

Biometric recognition for personalized HMI and IIoT implementation is difficult to realize in the cases of most existing machinery where there is a lack of the necessary equipment to operate in a smart manufacturing. This problem is more felt in Small and Medium Enterprises (SMEs) whose machinery renewal requires high investments that are not easy to sustain [8]. Smart retrofitting practices were born to precisely answer the SMEs' need to face the digital transformation while keeping costs under control.

Smart retrofitting means integrating a smart technology, initially not foreseen by the manufacturer, into an existing product. This makes it possible to adapt the machinery to an evolved and technological context of use, thus increasing its life cycle even with a minimal economic intervention, or in any case less than the adoption of a new machinery. This practice is of extreme importance, as it allows us to optimize the productive resources that are already available. In a nutshell, it represents the first step that a small or medium-sized company can take to embrace the concepts of Industry 4.0. Smart retrofitting can obviously try to cover any of the key aspects of Industry 4.0. It can, for example, allow machines to be equipped with the necessary sensors for fault prediction, it can enable a connected network among all machines to optimize production or add further safety measures.

This paper proposes an approach to embed biometric data-based authentication technologies in order to increase security and efficiency of legacy machines. To succeed in this objective, a technological system was developed: it is inspired by smart retrofitting and acts as the enabler to integrate biometric authentication on legacy machines. Despite the considerable interest in authentication using biometric data in the context of Industry 4.0, literature lacks examples of integration of such technology on legacy industrial machinery. Such integration can lead to a positive impact on machinery on-board safety and on the quality and usefulness of the log file created by the machine, going to solve the previously illustrated issues. In this way, the concepts introduced by Industry 4.0 such as efficiency, security, digitization, and interconnection are embraced, the first two by the introduction of biometric recognition, the last two by the remote management of a log file, now more accessible and manageable.

Human Factors, despite being referred to as one of the pillars of Industry 4.0, are little addressed when not entirely left out when considering smart retrofitting. Therefore, to ensure that they are placed at the heart of the matter, the development of the user interface was driven by guidelines (e.g., Ten Usability Heuristics by J. Nielsen) and best practices to ensure an appropriate usability. The results of the application of such principles were then verified through testing with real users. Moreover, the proposed system enables individualized HMI technologies, also meeting the paradigms of Industry 5.0, particularly to adopt a human-centric approach by means of artificial intelligence.

The system has been structured following a modular approach. In order to be applicable in every productive context (from SMEs to large corporations) its minimum configuration presents three modules (Authentication tool, Industrial PLC and Enterprise Server) but it can be expanded at will. The system scalability is virtually unlimited.

The rest of the paper is structured as follows: Chapter 2 illustrates the related works, while Chapter 3 describes the proposed system, its structure, and its features. Chapter 4 proposes a case study in which the proposed system has been applied to investigate its application in a real manufacturing environment. Chapter 5 follows with the discussions and finally Chapter 6 draws the conclusions and discusses the limitations of the present research work.

2 Related works

The General Data Protection Regulation GDPR 2016/679 defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data". The five best known and most popular technologies to retrieve biometric data are fingerprint reading, palm scanning, face recognition, iris recognition and finally voice recognition. Sonkamble et al. [9], proposed a benchmark among these technologies adopting five evaluative metrics: Universality, Uniqueness, Permanence, Performance and Measurability. The author assigns them a judgment that goes from L(ow) to H(igh). Elaborating the author's findings considering state-of-the-art advancements, face recognition technology proves to be the most promising technique.

In fact, converting the rating into a numerical grade from 1 (L) to 3 (H), and adding up the individual scores for each technology, it's found that at the time of writing the previously mentioned article [9], the iris recognition and fingerprint reading technologies were, with 14 and 13 points respectively, in first and second place. These were followed, in third position, by face recognition with 12 points. However, considering the amount of time that has passed since the paper's publication, it can be assumed that performance is no longer so relevant, due to the improved computational capabilities of modern PCs. Not taking performance into consideration, iris and face recognition are equal in merit with a score of 11, while fingerprint reading only scores 10 points. Analyzing the individual metrics, face recognition receives a higher score in measurability than iris recognition. Vice versa, face recognition is lower than its competitor in permanence, given that as the individual ages, face's traits undergo a more marked transformation than those of the iris. Despite this, however, according to a study by Best-Rowden et al. [10], face recognition accuracy only decreases by 0.01% over 6 years in 99% of subjects tested, without gender, race or age affecting the result. This translates into a decrease of 0.05% over a hypothetical 30-year long working life or 0.08% over 48 years, a decrease that proves to be completely negligible. The scores are shown in Table 1.

However, just considering the scores is not enough to state which of these technologies could be the best choice in the specific context of use analyzed in this article, namely the manufacturing environment, and more practical considerations and other more pragmatic aspects should be taken into account. First, fingerprint reading and palm scanning are prone to a common problem: workers of manufacturing companies almost always wear gloves, and although this is a problem that can be circumvented by removing the gloves when necessary, it would still slow down authentication operations. Therefore, in the search for a universally applicable authentication method, these two technologies should be discarded. Voice recognition should be discarded for another problem, also related to the application context. In fact, in a machine shop, audible sound noise may be too high and cover the worker's voice, preventing recognition.

Once again, face and iris recognition seem to be the best choices. However, as stated in [11], iris recognition is highly affected by the performance of the image capture hardware used to obtain iris pictures. While this biometric authentication technique can lead to great accuracy under ideal conditions (i.e. high imaging resolution, correct lightning conditions), drifting away from such ideal conditions has the effect of significantly decreasing recognition performances. Face recognition, instead, is nowadays performed using common RGB cameras such as USB webcams found in laptop PCs and smartphones. Moreover, iris recognition's performances can be affected by the user wearing glasses or contact lenses [12]. Finally, on the software projects online hosting service Github [13] a search with the keywords "face recognition" returns 3401 results, which drop to 32 in the case of the words "iris recognition". These results demonstrate how face recognition technologies absorb more interest in academic and software development fields than iris recognition. While it may therefore be of interest to explore the application of iris recognition, face recognition appears to be supported by a broader community of developers and researchers, resulting in a wider availability of ready-to-use software projects, including those of an open source nature.

Face Recognition (or FR, the act of associating a recognized face within the image with a real identity) is only the second step of a larger process, whose first step is Face Detection (or FD, i.e., identifying a face and if present localizing it within an image) and is usually associated with Deep Learning algorithms.

Adopting a CNN (an artificial neural network widely used for these kinds of tasks and generically for Deep Learning problems) to perform FR means decomposing the problem "locating a face in the frame" into simpler subproblems, such as "locating two eyes in the frame", "locating a mouth in the frame", and so on. These subproblems, then, can in turn be decomposed, such as looking for the presence of an eyelid, eyelashes, and eyebrows to determine the presence of an

Table 1 Comparison between the five most known biometric technologies

Biometric technologies	Universality	Uniqueness	Permanence	Performance	Measurability	Tot	Tot w/o Performance
Iris recognition	H (3)	H (3)	H (3)	M (2)	H(3)	14	11
Fingerprint reading	M (2)	H (3)	H (3)	H (3)	M (2)	13	10
Face recognition	H (3)	H (3)	M (2)	L (1)	H (3)	12	11
Palm scanning	M (2)	M (2)	M (2)	M (2)	H (3)	11	9
Voice recognition	M (2)	L (1)	L (1)	L (1)	M (2)	7	6

eye. This is made possible by the layered structure of a CNN, which adopts a more or less large number of hidden layers, with the aim of approaching the problem of identifying a face through an analysis carried out at the level of the single pixel. Some examples of CNNs applied to FR, but also to eye-gaze tracking, can be found in [14–17]. In these cases, the same and other information useful for the purpose of this paper are extracted (gender, age estimation, eye-gaze tracking, and FR), although they are applied to User Experience (UX) analysis.

Smart retrofitting, as defined by Jaspert et al. [18] is described as “the integration of new technologies and sensors into legacy systems, supporting the transition towards real smart manufacturing. It can extend the life cycle of machinery and equipment in a way that is feasible, time-saving, and requires comparatively low investments”. Thus, through smart retrofitting, one can pursue the goals of Industry 4.0 while not being equipped with state-of-the-art machinery, keeping adaptation costs low [19] while extending the life cycle of already acquired machinery [20]. Both aspects benefit, especially, small and medium-sized companies. In addition, it reduces the downtime [21] of equipment needed to adapt to new industrial paradigms. From this point of view, smart retrofitting can also be attractive to large companies, which would also have the economic capacity to carry out a more extensive renovation, but which are still careful to keep up with production. A literature search gives an idea of the purposes for which smart retrofitting is applied: (1) to increase the connectivity and intelligence of old robotic arms or CNC milling machines [22] (2) to equip a manufacturing plant, consisting of old machinery, with cloud computing capabilities [23] (3) to increase productivity and efficiency and to reduce energy consumption [24]. Even considering other works [25–27], the benefits that are aimed at implementing smart retrofitting fall into the four categories identified by Jaspert, namely: Sustainability, Functionality, Compatibility and Viability. However, this means forgetting one of the pillars of Industry 4.0: Human factors.

This work aims to fill the literature gap, presenting a system capable of increasing production efficiency, reducing the downtime required for authentication of the machine’s operators and keeping traceability of log-in and log-out, but also the safety of operators, preventing unauthorized personnel from intervening on the machine. The proposed objectives will be achieved by adopting user authentication through the reading of biometric data, namely with Face Recognition. This authentication process will be performed by means of a device, designed based on the system proposed here, which will allow to integrate the technologies discussed on machines that would otherwise be considered obsolete.

3 The proposed system

In this paper a new system using the retrofitting principles to introduce a more robust authentication mechanism on a legacy machine, with the possibility of improving the management and control of employees for security issues, is proposed. Using biometric data of the face as an access password, thanks to Face Recognition techniques, it is possible to recognize the identity of the users directly for on-board applications. In this way, thanks to the user profiles recorded and catalogued (based, for example, on the user’s role) directly on site and at the same time as the first access, it is possible to communicate to the machine who is interacting with it at that moment and for which areas of the machinery, whether hardware or software, the person in question has the access permissions.

In this article a first Use Case to test the developed application has also been described: this procedure involves the development of an on-board software for an employee authentication designed around three user typologies with

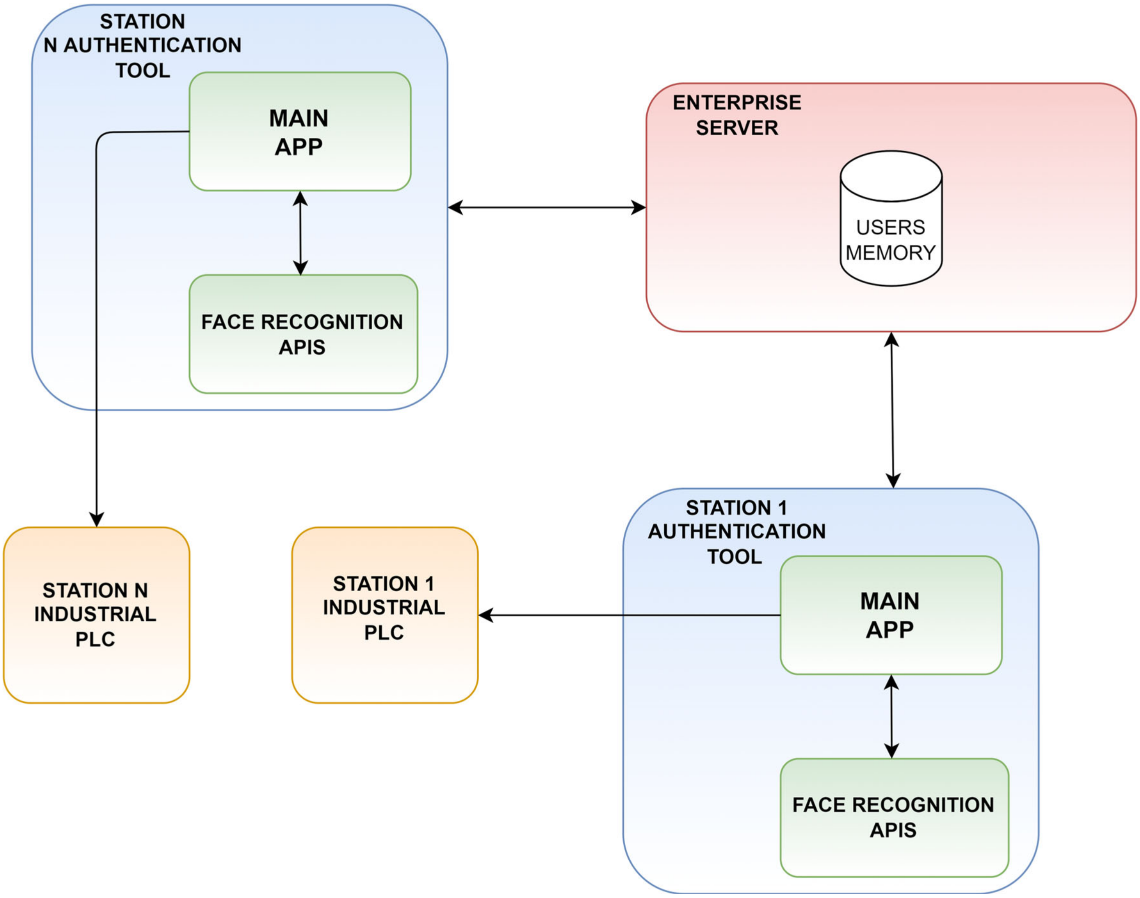


Fig. 1 The proposed system's modular architecture

different access profiles (Operator, Maintainer and Administrator).

3.1 The system design

The developed software, as previously mentioned, has the task of authenticating and granting access to an industrial PLC using advanced AI-based technologies to improve security, record any access and provide a readable and simplified method of accessing and reading logs.

First, the software must be able to distinguish between the different categories of users it may encounter and ensure that each one has the appropriate permissions (e.g. operator, maintainer, administrator). User flows could be defined following a User Story Mapping procedure. Going into more detail, the software allows a fast but above all reliable log-in procedure (i.e. any problem with the face recognition system does not compromise access), enabling the communication with a PLC and with the company's management team regarding the machine's operational status (in operation or in maintenance) and the user working on, and giving the user with the highest permission level (the administrator) the possibility to quickly access a logged-in users list. The used architecture gives the companies the flexibility that allows them to customize the log file as they wish, greatly improving its readability.

An architectural diagram of the system has been defined, shown in Fig. 1. According to the architectural scheme, the main modules are:

- *Authentication tool* the main software made up of a sub-module that manages GUI and logic of the whole application and of the Facial Recognition apis. This tool will be present for each workstation where authentication needs to be managed
- *Industrial PLC* the PLC that manages the industrial machine and enables access to it. The access data packet will be sent by the Main App once authentication is successful
- *Enterprise server* the server that can be contacted from the local network. From a centralised point of view, if there are more than one PLC to manage, this computer handles the only memory (not counting any backups) with QR images,

access credentials and generic user information, as well as the numerical encodings of the employees faces for which facial recognition consent has been given

3.2 The face recognition software implementation

For the implementation of the facial recognition APIs, the Python programming language, particularly suitable for Machine Learning tasks, and in this particular case Deep Learning tasks, has been used. For this module, the approach used in [28] and based on Deep Learning techniques has been used. In particular, this task requires two phases:

- A Registration phase, in which an image of the user's face, processed with the Dlib library facial detector [29], is converted into 68 facial landmarks coordinates and 128 values indicating the characteristic distances between them are stored on the server database to be used as reference
- A Recognition phase, in which the system activates the face recognition procedure several times. It is based on the open-source Python library face_recognition [30], chosen for two reasons:
  - It is capable of achieving 99.38% accuracy when tested on the Labeled Faces in the Wild benchmark [31]
  - It is a lighweight library that does not demands high computational resources, and can be implemented in low-cost hardware platforms such as a Raspberry Pi 2 +

Every time, following the approach defined by [30], it finds the characteristic facial distances and compares them with the ones stored on the database. The fault tolerance threshold is set at 0.6, and in case it gets crossed, the face recognition will fail. To make the system stricter, it is possible to reduce the threshold, but the algorithm becomes computationally heavier.

This system is also able to detect liveness. Many methods have been implemented in literature about this topic [32]. This is useful to avoid people from using photos during the authentication stage, in this way users cannot falsify their identity or mislead the system when it performs the face recognition. There are multiple factors involved in this control, for this research the Dlib 68 face landmarks are found, then any movement is exploited to prove the liveness of the user's face. In particular, the algorithm saves every 3 s the x and y coordinates of all the landmarks. Since the face might move and its size might change, the coordinates are normalized according to the width and height of the face. In this way, the system can compare the actual output with the one recorded 3 s before, detect movements, and thus, liveness. As Fig. 2 shows, each landmark (in green) is compared with the respective one of 3 s before (in red).

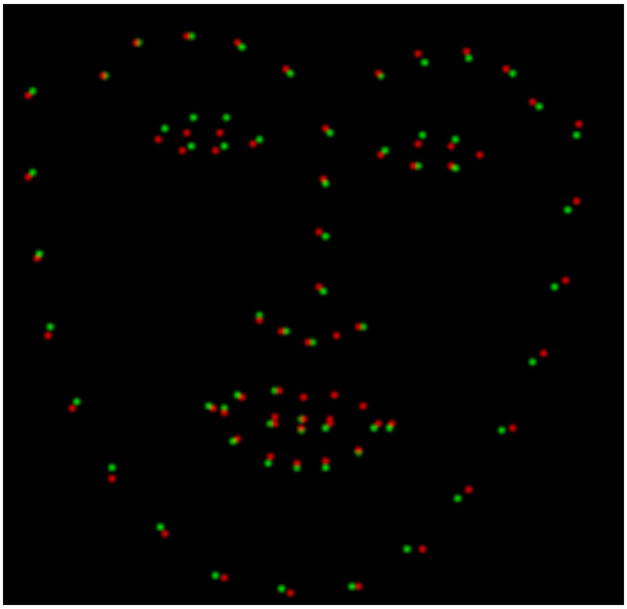


Fig. 2 Liveness detection landmark comparison

Lastly, another movement to detect the face's liveness is the eye blink. In particular, the algorithm finds facial landmarks, as shown in Fig. 3, and checks if the ratio between the height and the width of the eye changes. Therefore, the algorithm checks if there has been any eye blink in the last 3 s, and if that is verified, the liveness is detected.

Of course, occlusions, inadequate hardware or adverse ambient lighting issues (i.e. low light, light reflections, etc..), the user could denying consent to the processing of his photo may constitute issues for the face recognition software. Hoang et al. [33], proposes to circumvent the problem of occlusion or adverse light by adopting a mixed identification system between Facial Recognition and RFID tags. However, this solution, although effective, introduces the compromise of forcing the user to have always with him the RFID tag needed for the two-step authentication.

Instead, this research proposes a similar solution, with the generation of an identifying QR code during the user's registration, to be used later as an alternative access method. The QR code can either be stored inside the user's smartphone memory as an image or printed on a badge. In any case, a copy of the QR code is saved in a database at the disposal of the administration, to be used if necessary. Despite a decrease in security respect to the exclusive use of facial recognition technologies, the probability that it could be shared among unauthorized people, is low, being it tied to the owner's identity. Finally, where available, it will be advisable to provide an adequate system for the subject's illumination, so as to avoid at least the problem of poor ambient lighting.

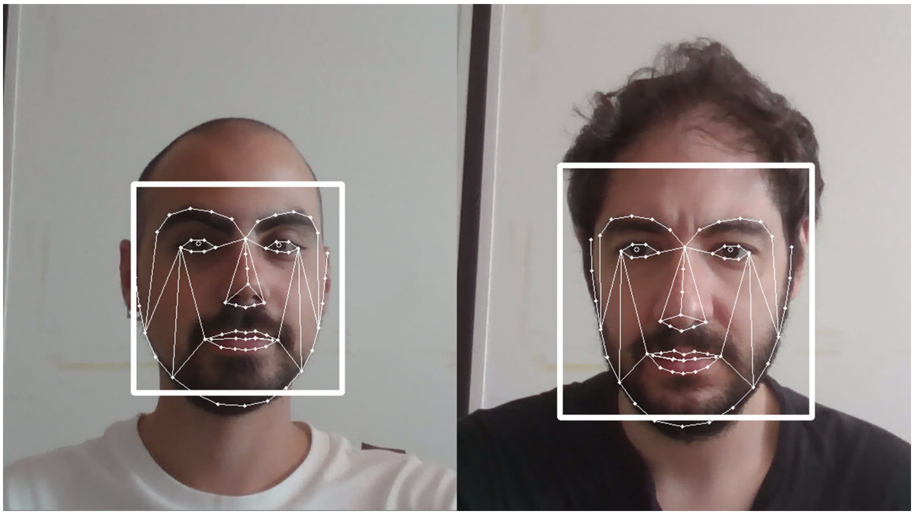


Fig. 3 Landmarks used by the Dlib landmarks predictor

4 Case study

4.1 Device design

The following hardware configuration has been chosen for the case study:

- Raspberry Pi 4 Model B 8 GB RAM
- Touchscreen display with an IPS 1920 × 1200 10.1″ panel
- Embedded webcam with 1080p resolution
- Led chain lights 12 V for user's face illumination

This configuration has been used to set up a totem installed in a medium-sized company operating in the field of design, production and sale of machinery and systems for industrial automation. The use of a Raspberry made it possible to obtain good computing performances and at the same time high portability with low costs. One of the main aims of the tool design and development was to obtain a good trade-off between increased security in authentication procedures and speed/simplicity of use, thus giving importance also to the usability.

For this use case the following architectural constraints has been defined, however the followed modular approach places no limits for the used communication protocols:

- Use of the Ethernet/IP protocol for communication with the industrial PLC
- Use of the FTP protocol for communication with the centralised company server
- Possibility to work without an external access to internet

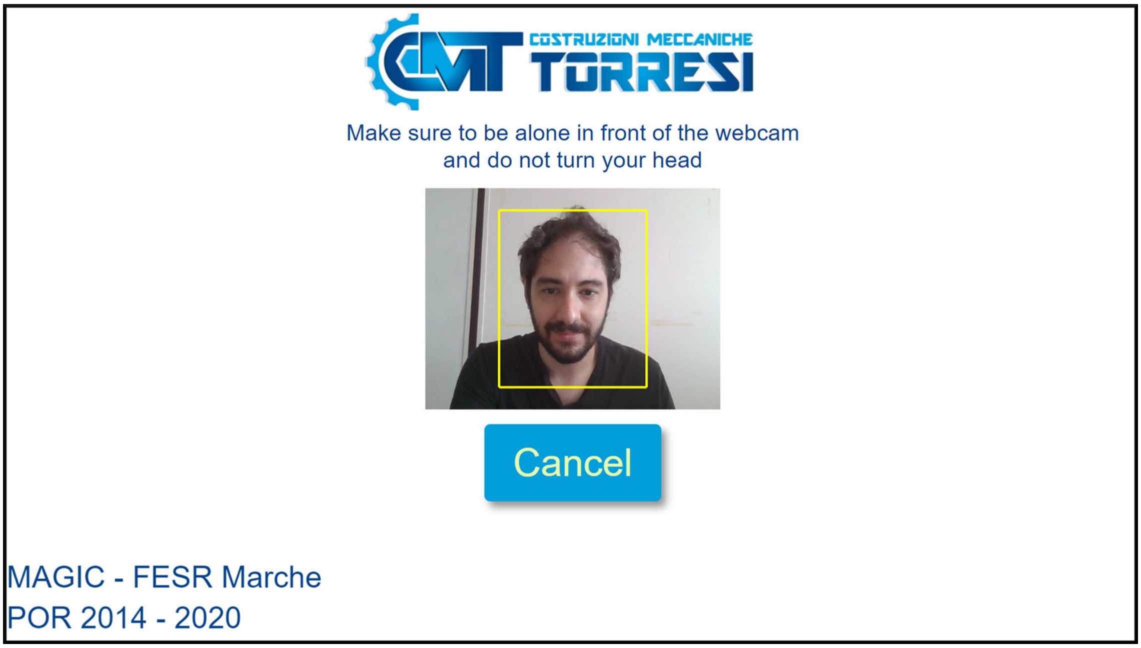
The defined user flows are three: administrator (with the highest permissions, capable of registering other users in the system and viewing who is logged-in and where in real-time), the maintainer (with mid-level permissions) and the operator (the one with only basic permissions).

For the development of the main software, the Electron framework was used, as it allows the development of desktop apps by working with the client languages of web programming (i.e. html, javascript and css). The face recognition module functionalities are then made available through dedicated REST APIs, contactable from the main app in Electron by means of simple HTTP calls.

In the registration phase (Fig. 4), the face-api.js library [34] has been used. This library provides different APIs for face detection, recognition of facial expressions, gender, and age, using models trained with the Tensorflow-lite framework for Javascript. Although these APIs are computationally light, they are often not as accurate, so they have only been used to give indications to the user on whether their face is recognisable by a face detection model (i.e., if they are maintaining a correct angle of the head and that the environmental conditions are suitable for face recognition).

Regarding the information produced during a user's registration (QR code image, authentication credentials and face encodings for facial recognition) and the authentication logs, the csv format was chosen while, as mentioned, the FTP protocol has been used for communication between the Electron app and the company server. If, for example, an administrator decides to authenticate himself using a QR code during a user's registration, the app will make a request to the server via FTP and will download the list of all the UUID codes decoded from the QRs themselves and saved in a csv file. If the UUID code associated with the QR presented during authentication does not match any of those in the csv file, the software will block the access and automatically return to the home page of the registration section.

Similarly, if the software did not recognize the user during the facial recognition phase (by making associations in a



Make sure to be alone in front of the webcam and do not turn your head

MAGIC - FESR Marche
POR 2014 - 2020

Fig. 4 An overview of the device's interface while performing Face Recognition

similar way with all the encodings stored in the csv file), the user will automatically find himself back in the home of the authentication section.

4.2 Evaluation metrics

All the tests described below took place in various SMEs which are partners of the company that supported the research project, and 20 of their employees were involved (age: 38.57 ± 19 years, 12 females and 8 males). All the test procedures were performed in compliance with EU privacy laws (GDPR) and institutional guidelines.

The first test assessed the accuracy of the Face Recognition software. To conduct the accuracy test, 15 of the subjects were registered in the software and the other 5 were not. Then, each one performed a face recognition test at about 11:00 am, with well distributed natural light, and another one at 5:00 pm on an autumnal day, with artificial light, for a total of 40 tests. The outcome was recorded, distinguishing them into four categories:

- True positives (TP), if the software correctly attributes an identity to the face to be recognized
- False positives (FP), when the software attributes a wrong identity to the face to be recognized
- True negatives (TN), i.e., when the software does not attribute an identity to a face shown to it because it does not actually belong to the set of previously recorded faces
- False negatives (FN), finally, when the software does not attribute an identity to the face despite it belongs to the set of recorded faces

Then, the effectiveness of the proposed system was tested. As a first step, an interview has been conducted with the department heads and production managers of the involved SMEs. Through this tool, we assessed the issue of unauthorized access made possible by old authentication procedures. The questions composing the interviews were two:

- Can you estimate an overall percentage of unauthorized access compared to total access?
- What are the indicators that allowed you to estimate this percentage?

Going further, several use tests were performed. Subjects were asked to perform four procedures:

- Log-in via Face Recognition
- Log-in via QR code
- Log-out via Face Recognition
- Log-out via QR code

To measure the objective effectiveness of the proposed system, the task completion time was measured during the course of the tests, as well as the number of errors made was noted. Then, these measurements were compared with the usual access times for the old authentication implemented

Table 2 Confusion matrix with data obtained from the accuracy test

	Positive	Negative
True	24 (60%)	13 (32.5%)
False	0 (0%)	3 (7.5%)

systems, calculated as the average value in seconds from 10 conducted tests.

Finally, usability was assessed. As far as the objective usability's aspects, the times and errors previously measured for the proposed system are now compared with the same ones but measured with expert users (i.e. the designers of the system). Viceversa, to address the subjective aspects, participants were asked to complete the SUS questionnaire [35] at the end of the test.

4.3 Results

The data obtained from the Facial Recognition accuracy test were organized into the confusion matrix reported in Table 2 (with quantities for each outcome indicated).

The accuracy was calculated as in Eq. 1:

$$ACC = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (1)$$

showing a final value of 92.5%.

The interview conducted with the department heads and production managers showed that unauthorized access, prior to our intervention, amounted to about 70% of the total, across all the interviewed SMEs. This data is, of course, the results of a rough estimation and so is highly empiric, as it cannot be precisely measured. However, this rough estimate stems from the observation made by interviewees regarding machines downtime due to incorrectly set parameters. Assuming that an experienced person would not have set these values, it is concluded that those who made these changes did not have the necessary training and therefore, most likely, did not have the authorization. Unfortunately, the SMEs have not communicated the exact numerical data for reasons of corporate secrecy.

After some preliminary tests over the arc of two months, it is verified that the proposed system greatly prevents this risk. In fact, machine's downtimes have reduced by about 60% compared to before the adoption of the device. Moreover, the device now allows to check who was logged-in when the downtimes occurred: thanks to the log file, it has been verified that every time a machine stopped working due to a wrong parameter setting, the person who was logged-in was in fact authorized to do so.

Further on, the measurements of the time taken on the old systems to request and obtain machine access show an average of 41.5 s (Standard Deviation, SD = 21.1 s). Thanks to the proposed system, this average is reduced to 14.28 s (SD = 3.96 s) in case of a Face Recognition log-in procedure or 12.33 s (SD = 5.71 s) in case of a QR log-in procedure. Thanks to the integrated subject illumination system, authentication is successful even in low illumination conditions. With the proposed system, the access is obtained with personal data (i.e., the face of the subjects or their QR) and so the user traceability is granted. The log-out procedures showed similar results, with a time to log-out via Face Recognition of 15.58 s (SD = 2.52 s) and 20.05 s (SD = 21.66 s).

Similarly, the average number of errors with the old authentication system amounts to 1.5 errors per day and is reduced to 0 errors with the proposal of this paper, except for the QR log-out procedure, which shows an average of 0.14 errors (SD = 0.35 errors). The results are summarized in Fig. 5.

For the usability tests, expert users finished their tasks with the following time and errors:

- *Log-in via face recognition* 14.59 s (SD = 0.59 s) and 0 errors
- *Log-in via QR code* 13.12 s (SD = 2.12 s) and 0 errors
- *Log-out via face recognition* 15.08 s (SD = 1.93 s) and 0 errors
- *Log-out via QR code* 8.79 s (SD = 0.79 s) and 0 errors

The comparison between the two sets of data is shown in Fig. 6.

Finally, the SUS questionnaire median results (and their standard deviations) are shown in Table 3.

5 Discussion

The Face Recognition accuracy test, performed in the wild directly on workplaces instead of a controlled environment such as a laboratory, showed remarkable results. Thanks to its high accuracy, this software does not act as a bottleneck for the general performance of the authentication system. Moreover, such high accuracy has been later confirmed over the arc of the two months of tests, where the device has been used by the involved SMEs directly in production, although for non-critical activities. If not for rare occasions (where, anyway, the use of a backup authentication system such as QR code reading has assured the continuity of the operations) the Face Recognition software did not cause any particular problems.

Further on, over the arc of these two months of continuous use, a complete elimination of illegal access, to the best of

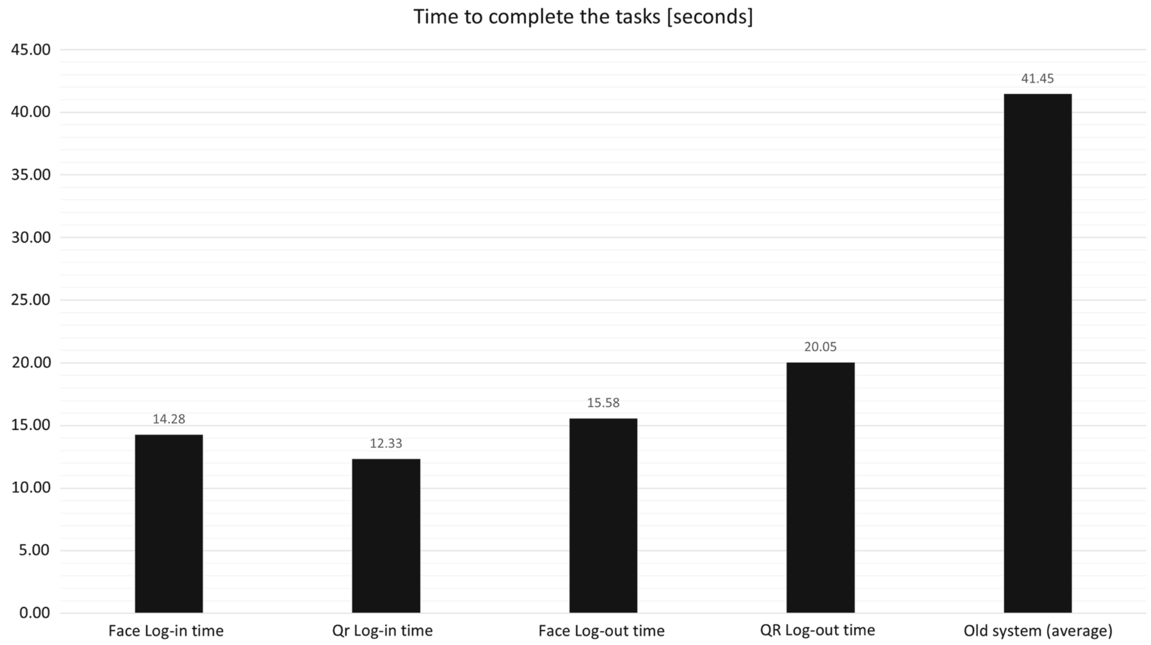


Fig. 5 Comparison of the times needed by the subjects to obtain machine access on the proposed system and on the old system

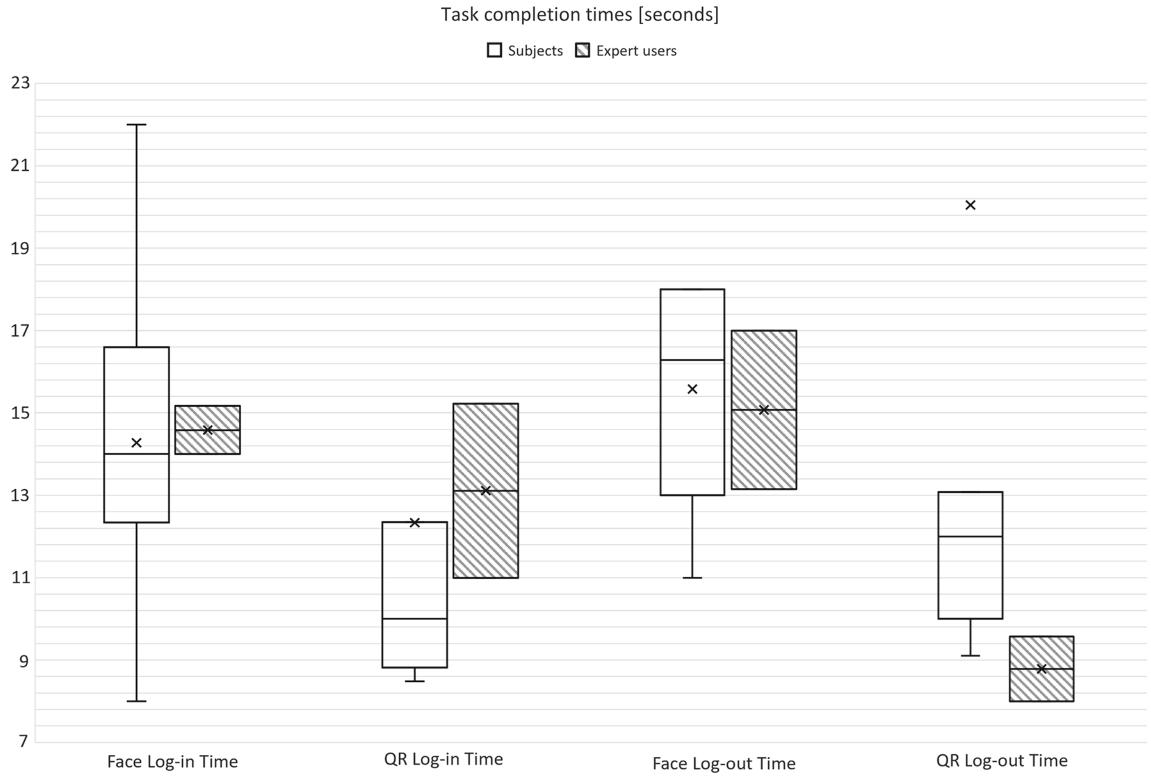


Fig. 6 Comparison of the times needed by the subjects and by the expert users to login and logout with the proposed system

Table 3 SUS median score and relative standard deviations

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
SUS Score	4.00	1.00	5.00	1.00	5.00	1.00	4.00	1.00	5.00	1.00
SD	0.70	0.45	0.35	0.00	0.45	0.35	0.49	0.00	0.45	0.35

our knowledge, has been achieved. The remaining machine's downtimes are now just attributable to human errors.

Finally, a careful design of the User Interface allowed to reduce at minimum the slowdowns due to a wrong use of the system. In fact, times obtained by the subjects show a complete comparability against those obtained by the expert users (i.e., the designers). In one case (QR Log-in) the subjects' times are even lower than those of the designers, while in another one (QR Log-out) a considerably high time of only one subject shifted upwards the average time, albeit slightly. The other two cases (Face Log-in and Face Log-out) are fully comparable between the two sets of data. Such easiness of use of the system is also supported from the SUS questionnaire's results, given they show an essentially positive judgement on all of the ten questionnaire's categories.

6 Conclusions

This research project proposes a retrofitting approach based on the application of deep-learning and computer vision technologies for facial recognition to improve access to machinery in mainly manufacturing contexts.

The major limitation of the proposed study is the empirical nature of one of the main issues it aims to solve, i.e. the amount of illegal accesses compared to the overall number of accesses. Although, in fact, these data derive from a decade of experience of the supporting partner with its customers, there is still a certain degree of uncertainty in the numerical data. The problem arises from the fact that, today, there is no system able to track the workers identity with legacy systems, so the only useful tools to estimate the number of illegal accesses are interviews and inferences derived from the observation of other quantitative phenomena, more or less related. A future study could compare the situation regarding machine downtime due to incorrect parameters pre-adoption of the device with that post-adoption, observing the data for a sufficiently long period of time.

Possible future developments will include the possibility of testing the behaviour of the system in a production environment once it will be implemented following architectural choices more in line with this purpose. These changes will undoubtedly involve the use of more performing hardware systems, communication protocols and software frameworks, thus replacing the Raspberry with an industrial mini-computer and using lower-level frameworks and languages such as C + + . Moreover, a further limitation comes from the currently integrated liveness detection system. In fact, although keeping track of the relative micro-movements between the landmarks or of eyes blinking allows to effectively distinguish a real face from a static image, if someone tries to use a video shot to carry out the authentication the system would not be able to make the distinction. A possible future study, aimed to further improve security, could use a combination of an RGB camera with infrared grids projected onto the face to be recognized, in a similar way to what happens with Microsoft Windows Hello or Apple Face ID. The proposed system serves as an enabling technology to introduce one of the paradigms of Industry 5.0, to adopt a human-centric approach by means of artificial intelligence. In fact, the adoption of Face Recognition technologies is the first step toward the implementation of further features such as, for example, Facial Coding to analyze the user's emotions and cognitive load so as to decline the user interface on them. Finally, what is proposed in this paper represents a pragmatic solution for those production realities really interested in taking the first steps towards a Human Centered approach.

Acknowledgments MAGIC: Research and development of a novel haptic user interface with a customizable aesthetics to control human-aware living environments, POR MARCHE FESR 2014-2020 - ASSE 1 - OS 1 - AZIONE 1.1.INT 1.1.1 and supported by Costruzioni Meccaniche Torresi Srl.

Funding Open access funding provided by Università Politecnica delle Marche within the CRUI-CARE Agreement. The funding was provided by Regione Marche.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Schmidt, R., Möhring, M., Härting, R.C., Reichstein, C., Neumaier, P., Jozinović, P.: Industry 4.0-potentials for creating smart products: empirical research results. In International Conference on Business Information Systems, pp. 16–27. Springer, Cham. (2015) https://doi.org/10.1007/978-3-319-19027-3_2
2. Weyer, S., Schmitt, M., Ohmer, M., Gorecky, D.: Towards industry 4.0-standardization as the crucial challenge for highly modular, multi-vendor production systems. Papersonline **48**(3), 579–584 (2015). https://doi.org/10.1016/j.ifacol.2015.06.143
3. Boyes, H., Hallaq, B., Cunningham, J., Watson, T.: The industrial Internet of Things (IIoT): an analysis framework. Comput. Ind. **101**, 1–12 (2018). https://doi.org/10.1016/j.compind.2018.04.015
4. Calabrese, M., Cimmino, M., Manfrin, M., Fiume, F., Kapetis, D., Mengoni, M., Toscano, G.: An event based machine learning framework for predictive maintenance in industry 4.0. In: International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Vol. 59292, p. V009T12A037. American Society of Mechanical Engineers. (2019). https://doi.org/10.1115/DETC2019-97917.
5. Calabrese, M., Cimmino, M., Fiume, F., Manfrin, M., Romeo, L., Ceccacci, S., Kapetis, D.: SOPHIA: an event-based IoT and machine learning architecture for predictive maintenance in industry 4.0. Information **11**(4), 202 (2020). https://doi.org/10.3390/info11040202
6. Rueckert, U.: Human-machine interaction and cognitronics. NanoChips **2030**, 549–562 (2000). https://doi.org/10.1007/978-3-030-18338-7_28
7. Colasante, A., Ceccacci, S., Talipu, A., Mengoni, M.: A fuzzy knowledge-based system for diagnosing unpredictable failures in CNC machine tools. Proc. Manuf. **38**, 1634–1641 (2019). https://doi.org/10.1016/j.promfg.2020.01.121
8. Jimeno-Morenilla, A., Azariadis, P., Molina-Carmona, R., Kyratzi, S., Moulianitis, V.: Technology enablers for the implementation of Industry 4.0 to traditional manufacturing sectors: a review. Comput. Ind. (2021). https://doi.org/10.1016/j.compind.2020.103390
9. Sonkamble, S., Thool, D.R., Sonkamble, B.: Survey of biometric recognition systems and their applications. J. Theoret. Appl. Inf. Technol. **11**
10. Best-Rowden, L., Jain, A.K.: Longitudinal study of automatic face recognition. IEEE Trans. Pattern Anal. Mach. Intell. **40**(1), 148–162 (2017). https://doi.org/10.1109/TPAMI.2017.2652466
11. Al-Waisy, A.S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., Nagem, T.A.: A multi-biometric iris recognition system based on a deep learning approach. Pattern Anal. Appl. **21**(3), 783–802 (2018)
12. Majekodunmi, T.O., Idachaba, F.E. (2011). A review of the fingerprint, speaker recognition, face recognition and iris recognition based biometric identification technologies
13. Github. https://github.com/. Accessed 9 Feb 2022
14. Talipu, A., Generosi, A., Mengoni, M., Giraldi, L.: Evaluation of deep convolutional neural network architectures for emotion recognition in the wild. In: 2019 IEEE 23rd International Symposium on Consumer Technologies (ISCT), pp. 25–27. (2019). IEEE
15. Generosi, A., Altieri, A., Ceccacci, S., Foresi, G., Talipu, A., Turri, G., Giraldi, L.: MoBeTrack: a toolkit to analyze user experience of mobile apps in the wild. In: 2019 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–2. IEEE (2019) https://doi.org/10.1109/ICCE.2019.8662020.
16. Ceccacci, S., Generosi, A., Giraldi, L., Mengoni, M.: An emotion recognition system for monitoring shopping experience. In: Proceedings of the 11th PErvasive Technologies Related to Assistive Environments Conference, pp. 102–103. (2018) https://doi.org/10.1145/3197768.3201518
17. Generosi, A., Ceccacci, S., Faggiano, S., Giraldi, L., Mengoni, M.: A toolkit for the automatic analysis of human behavior in HCI applications in the wild. https://doi.org/10.25046/aj050622
18. Jaspert, D., Ebel, M., Eckhardt, A., Poeppelbuss, J.: Smart retrofitting in manufacturing: a systematic review. J. Clean. Prod. (2021). https://doi.org/10.1016/j.jclepro.2021.127555
19. García, J.I., Cano, R.E., Contreras, J.D.: Digital retrofit: a first step toward the adoption of Industry 4.0 to the manufacturing systems of small and medium-sized enterprises. Proc. Inst. Mech. Eng. Part B: J. Eng. Manuf. **234**(8), 1156–1169 (2020). https://doi.org/10.1177/0954405420904852
20. Guerreiro, B. V., Lins, R. G., Sun, J., Schmitt, R.: Definition of smart retrofitting: First steps for a company to deploy aspects of industry 4.0. In: Advances in Manufacturing, pp. 161–170. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-68619-6_16
21. Kim, D.Y., Park, J.W., Baek, S., Park, K.B., Kim, H.R., Park, J.I., Baek, W.: A modular factory testbed for the rapid reconfiguration of manufacturing systems. J. Intell. Manuf. **31**(3), 661–680 (2020). https://doi.org/10.1007/s10845-019-01471-2
22. Arjoni, D.H., Madani, F.S., Ikeda, G., Carvalho, G.D.M., Cobianchi, L.B., Ferreira, L.F., Villani, E.: Manufacture equipment retrofit to allow usage in the industry 4.0. In: 2017 2nd International Conference on Cybernetics, Robotics and Control (CRC), pp 155–161. IEEE. (2017). https://doi.org/10.1109/CRC.2017.46.
23. Haskamp, H., Orth, F., Wermann, J., Colombo, A.W.: Implementing an OPC UA interface for legacy PLC-based automation systems using the Azure cloud: An ICPS-architecture with a retrofitted RFID system. In: 2018 IEEE Industrial Cyber-Physical Systems (ICPS), pp. 115–121. IEEE. (2018). https://doi.org/10.1109/ICPHYS.2018.8387646.
24. Alias, C., Salewski, U., Ortiz Ruiz, V.E., Alarcón Olalla, F.E., Neirão Reymão, J.D. E., Noche, B.: Adapting warehouse management systems to the requirements of the evolving era of industry 4.0. In: International Manufacturing Science and Engineering Conference, Vol. 50749, p. V003T04A051. American Society of Mechanical Engineers. (2017). https://doi.org/10.1115/MSEC2017-2611.
25. Bunterngchit, C., Pornchaivivat, S., Bunterngchit, Y.: Productivity improvement by retrofit concept in auto parts factories. In: 2019 8th International Conference on Industrial Technology and Management (ICITM), pp. 122–126. IEEE. (2019). https://doi.org/10.1109/ICITM.2019.8710655.
26. Givehchi, O., Landsdorf, K., Simoens, P., Colombo, A.W.: Interoperability for industrial cyber-physical systems: an approach for legacy systems. IEEE Trans. Industr. Inf. **13**(6), 3370–3378 (2017). https://doi.org/10.1109/TII.2017.2740434
27. Strauß, P., Schmitz, M., Wöstmann, R., Deuse, J.: Enabling of predictive maintenance in the brownfield through low-cost sensors, an IIoT-architecture and machine learning. In: 2018 IEEE International conference on big data (big data), pp. 1474–1483. IEEE. (2018). https://doi.org/10.1109/BigData.2018.8622076.
28. Ceccacci, S., Generosi, A., Cimini, G., Faggiano, S., Giraldi, L., Mengoni, M.: Facial coding as a mean to enable continuous monitoring of student's behavior in e-Learning. In teleXbe (2021)
29. King, D.E.: Dlib-ml: a machine learning toolkit. J Mach Learn Res **10**, 1755–1758 (2009). https://doi.org/10.5555/1577069.1755843
30. Face_recognition. https://github.com/ageitgey/face_recognition. Accessed on 23 Sept 2021
31. Labeled Faces in the Wild. http://vis-www.cs.umass.edu/lfw/. Accessed 9 Feb 2022

32. Chakraborty, S., Das, D.: An overview of face liveness detection. arXiv preprint arXiv:1405.2227. (2014) http://arxiv.org/abs/1405.2227
33. Hoang, V.D., Dang, V.D., Nguyen, T.T., Tran, D.P.: A solution based on combination of RFID tags and facial recognition for monitoring systems. In: 2018 5th NAFOSTED Conference on Information and Computer Science (NICS), pp. 384–387. IEEE. (2018). https://doi.org/10.1109/NICS.2018.8606895
34. Face-api.js. https://justadudewhohacks.github.io/face-api.js/docs/index.html. Accessed 14 Sept 2021
35. Brooke, J.: SUS: a retrospective. J. Usability Stud. **8**(2), 29–40 (2013). https://doi.org/10.5555/2817912.2817913

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.