HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Arnold ŐSZI – Lourdes RUIZ S
oszi.arnold@bgk.uni-obuda lourdes.ruiz@ bgk.uni-obuda.hu

BIOMETRIC USES IN OCCUPATIONAL SAFETY AND HEALTH

Abstract

Biometrics is used to recognize the identity of a specific individual using unique physical or behavioral traits such as: fingerprints, facial recognition, iris, gait, DNA, etc. Occupational safety and health (OSH) is a multidisciplinary field that focuses on recognizing, analyzing, preventing and minimizing risks in the workplace in order to provide health and safety to the employees. Biometrics and OSH are different study fields but share a common goal that is to provide enhanced safety. The following document identifies and describes conventional and potential uses of biometrics in the workplace, devices and technology relevant to OSH procedures and practices.

A biometrikus azonosítást egyének felismerésére alkalmazzák, felhasználva az egyéni fizikai és viselkedési jellemzőket, mint például az ujjnyomat, az arc felépítése, az írisz, a járás, a DNS, stb. A munkahelyi biztonság és egészségvédelem (OSH) egy multidiszciplináris terület, amelynek a középpontjában a munkahelyi kockázatok minimalizálására, felismerése, elemzése, megelőzésére áll, annak érdekében, hogy biztosítsa a biztonságot és az egészség megőrzését az alkalmazottak. A biometria és a munkavédelem egymástól különböző tanulmányi területek, de közös bennük, hogy a céljuk a nagyobb biztonság megteremtése. Az alábbi dokumentum beazonosítja és leírja a biometrikus eszközök hagyományos és a további lehetséges felhasználási területeit a munkahelyen, az eszközöket és a technológiákat, amelyek relevánsak a munkavédelmi szempontból kritikus eljárásokhoz és gyakorlatokhoz.

Keywords: *biometrics, occupational, safety, technology, health, uses, devices ~ biometria, munkavédelem, biztonság, technológia, egészség, felhasználás, eszközök*

INTRODUCTION

Biometrics is the science used to measure and analyze specific physical or behavioral traits in humans, in order to recognize the identity of a specific individual. Some of the characteristics used are: fingerprints, face, iris, voice recognition, hand geometry, gait, signature, DNA, odor [1]. Biometric systems are implemented to provide safety in various areas such as forensics, banking, airport control, electronical commerce, government social services and building accessibility. Biometrics technology poses a broad potential in other areas such as occupational safety. Occupational Safety and Health (OSH) is a multidisciplinary field that focuses in the recognition, analysis and prevention of hazards in the workplace. Its main goal is to protect workers by offering a healthy and safe work environment [2]. The purpose of this document is to identify conventional and prospective uses of biometrics in the workplace relevant to OSH practices.

Biometric systems focus on the concept that physical or behavioral characteristics in humans can be distinctive, for this reason it eases the identification of a specific person. These systems offer a high level of security compared with passwords or identification cards because they are based in the identification of a person using their inherited attributes that are unique. Biometric systems are based on pattern recognition which consists of two parts: enrollment and recognition. In the enrollment step, biometric traits are obtained from the individual, only distinctive features of the data collected are stored in the database. In the recognition part, biometric data is collected from the individual and compared with the data stored at the enrollment step in order to recognize and authenticate the person identity [1]. Biometric technologies offer an accurate verification where just an authorized person gets access to the information or place that is secured. Moreover, accountability is an advantage that can successfully identify a particular action or event to a person. It also prevents duplication, sharing of information and fraud, which provides a safer organizational environment.

OSH management systems concentrate in recognizing, addressing and preventing risks inside an industry aiming the welfare, health and safety of the employees. Moreover, the implementation of OSH practices contributes to the reduction and elimination of accidents, incidents, work related injuries and diseases. These systems involve the participation of the whole company and resources, including policies, processes, procedures, workforce and leadership at all levels of the organization [3].

Biometrics and OSH systems emphasizes in providing safety in different fields. Biometrics can be a powerful tool to be implemented in the workplace by providing access and correctly authenticate personnel identity. Biometric technology is becoming very popular among companies. Devices such as biometric time clocks and biometric physical access control readers had revenues of $225 million and $190 million in 2013 and it is expected to increase to $350 million and $ 300 million respectively in 2018 [4]. For this reason, it is important to distinguish the different occupational hazards and risks in an industry and therefore utilize biometric devices to protect workers and minimize accidents.

HAZARDS AND RISKS IN THE WORKPLACE

Hazards are present in every work environment. An occupational hazard is anything that has the potential to hurt or harm a worker. A risk is the likelihood or chance that the hazard will harm an employee [5]. Hazards are classified into two groups: safety hazards, cause accidents that can injure a worker and; health hazards, cause an occupational disease or illness, these hazards can be biological, physical, chemical, ergonomic, and organizational.

Safety hazards include conditions such as spill in the floors, blocked aisle, improper handling of cords in the floors, work from heights using ladders or in roofs, unguarded machinery, moving parts, electrical and confined spaces

Health hazards are subdivided into:

- Biological hazards involve the exposure to infected animals, people or plants by blood, bacteria, viruses and insect bites.
- Physical hazards include radiation, high exposure to ultraviolet rays, work at extreme temperatures, loud noise.
- Ergonomic hazards are the result of a type of work, body position or conditions that can affect the body. They can cause chronic diseases if there is a long term exposure. Some examples are inadequate workstations, frequent lifting, bad posture, repetitive movements, and vibration.
- Chemical hazards are present in cleaning products, paints, solvents, vapors, gases, flammable materials and pesticides.
- Organizational hazards comprise high workload, violence, lack of respect, flexibility, social support and sexual harassment [6].

HAZARD CONTROL

Controlling, managing and removing hazards imply a better work protection. Exposure is a main factor that needs to be considered in order to reduce hazards. Hazard controlling methods are:

- Engineering approach consists of redesigning and modifying workspaces, processes and equipment towards the reduction of workers' exposure. This method is preferred because it works independently of the workers. Engineering controls includes: substitution, when a less dangerous material is used or a process is changed; isolation restricts the exposure of the people working directly with the hazard by the inclusion of a containment structure; and ventilation implies a local exhaust system that eliminates the contaminant in the air thus it is not dispersed in the workplace.
- Working procedures and hygiene during job activities.
- Administrative approaches such as job rotation, break cycles, maintenance procedures.
- Effective usage of personal protective equipment at work such as hard hats, hear protectors and protective clothing [5].

Biometric science is mainly used as an engineering approach. The implementation of biometric devices contributes to controlling and minimizing hazards in the workplace. It is also a powerful tool for providing enhanced security to employees and to the work environment. Biometric management systems offer a variety of safety solutions to companies; additionally they can be used in different processes along the supply chain.

BIOMETRIC USES

Biometric Systems have been specially used in three different aspects:

1. For commercial uses such authentication in online banking services or ATM, credit card usage, e-commerce, mobile phone, distance learning, access to health care systems, etc.
2. For government purposes such as issuing ID cards, driver's licenses, social benefits, homeland security.

3. For forensic uses such as body identification, criminal purposes, parenting determination and lost persons [1].

CONVENTIONAL USES OF BIOMETRICS IN THE WORKPLACE

Biometric Systems provide safety to companies and employees building a safe and healthy work environment. In addition, they serve for numerous purposes listed below:

- Background Check, employers use biometric technology at the beginning of the recruiting process. In United States (US), companies perform employment screenings to candidates looking for a job position. FBI retrieves the criminal story of the applicants which helps the recruiter regarding a hiring decision. FBI uses two biometric fingerprint and two name-based background check [7]. It is important to know about the criminal records of candidates and employees because depending on the criminal offense, it can be a threat to the organization and to the other employees. Therefore, employee screenings can enhance the security in a company.
- Monitoring Staff, fingerprint recognition devices are mainly used for recording employees' time. These devices have built-in software that calculates accurately the working hours, punctuality, breaks, sickness, absence, over time and payroll. Other devices can deny access to company technology and networks after finishing the workday. Workers can clock in and out just by using their fingerprints in a faster way than traditional methods such as passwords or magnetic cards. Fraud and buddy punching is effectively reduced using this technology which enhances workers efficiency and productivity [8].
- Access Control, biometric data based devices are used for recognizing and grant access to authorized personnel by the authentication of their identity using biometric traits such as fingerprints, face recognition and eye scanning. They provide an additional security against trespassers by protecting buildings, computers and networks. In addition, biometric recognition restricts access to specific areas in the workplace such as facilities that contain dangerous, valuable materials or sensitive information. Keyless locks that utilize biometric traits track access and workers' activities and also prevent the access of intruders which offer a safety organizational climate [9].
- Biometric devices usage is effective on tracking company's property such as vehicles. They can provide valuable information such as: real time data on speed, location and different variables such as time for delivering companies. These devices can offer a trustworthy traceability report along the working schedule that can be useful in case of accidents and for claiming responsibility [4]. Moreover, biometric technology can track the employee in the workplace at any time which controls misconduct and behavior. It also promotes safe conducts among workers and enhances the usage of safety procedures while performing the work tasks.

POTENTIAL USES OF BIOMETRICS IN THE WORKPLACE

Introduction of biometric technology in the workplace have different uses listed above but also contributes to the development of various potential uses intended for the protection of workers. Some of them are explained here:

- As part of a health management program, biometric measures such as: height, weight, body mass index, waist and hip circumference, body fat blood pressure and

pulse rate are collected from employees. Biometric screenings are useful to identify health risks, modification of behavior, for implementing educational programs and changes in the work environment and culture. The measures are part of a work health assessment in which the company evaluates the worker health through the time in order to prevent work related diseases, reduce health costs and improve workers' health and productivity. The extraction of the biometric data creates an employee health baseline to prevent and perform health interventions, refer to health specialists, generate specific health programs, create awareness and direct actions to improve workers' health [10]. Employee wellness program is taking into consideration by employers because of the variety of health benefits to the workers that are translated in reduction of costs and creation of a healthy and safe environment inside and outside the workplace.

- Devices used in the workplace such as laptops, USBs and mobile phones have fingerprint detector systems. These systems authenticate users and provide traceability during the whole usage of the equipment. Windows Hello is a Microsoft's biometric authentication feature that allows employees to have access to company's devices and networks by using fingerprint and facial recognition. It can be used by multiple users that work with the same device. This method is backed with a PIN which is safer against credential theft [11]. The potential use of this feature is that can be implemented in any type of machinery. In automated machinery, it is important to have a record of the employees using the equipment in different cases such as work hours, maintenance, calibration and repair. In operations such as a lock out for maintenance, just the authorized personnel can turn on the machinery offering a protection to other workers around. The machine can have multiple users that allow special features to each one ensuring the safety of the procedures and the product.

BIOMETRIC TECHNOLOGY AT THE WORKPLACE

Biometric equipment is used mainly for fingerprint and facial recognition at the workplace. Different companies are developing devices and software for providing enhanced security in the workplace. The technology described below is just some examples of the variety of biometric options offered to industries in order to fulfill their employees' biometric authentication necessities.

- uAttend is a company that designs employee management systems and manufacturers affordable biometric devices and a cloud-based software that tracks worker's time and attendance. The software works with different applications such as clock, smartphone apps and web monitoring systems in one interface. It comprises different features such as tracking and reporting of overtime, holidays, different departments inside the company, vacations, sick leave, breaks and payrolls. The company specializes in manufacturing time clocks with fingerprint and facial recognition. Table 1 shows fingerprint time clock BN500 and facial recognition time clock MN1000. These devices provide time keeping solutions to small and medium enterprises [12].
- Kronos Incorporated is a company that provides workforce management concerning workers' time and attendance. It offers biometric identification and recognition when the employee clocks in and out or work. Moreover, it has several software features that allow employers to track time, efficiency, productivity and compliance among the workforce. Table 1 shows Kronos InTouch time clock which provides biometric

identification to validate employees' identity. Kronos Inc provides tailored monitoring solutions to small, medium and large enterprises [13].

- Privaris Incorporated designs and provides biometric authentication mobile devices which grant access to buildings, offices, computers, networks, websites, before connecting with an existing security system which provides an additional protection against intruders. Plus ID is one of its main products; it consists of a personal fingerprint device and a secure processor, the device recognizes the user and releases an access code or credential. It can store different information such as entry codes, passwords, credit cards, licenses, photographic images and additional biometric data. It is compatible with Bluetooth and radio-frequency identification (RFID) systems. Table 1 shows Privaris Plus ID key fob. This device is a powerful tool in the workplace because it provides an all in one solution to security by granting access to the physical facilities in a company but also access to computers and networks. It enhances safety since it works by the recognition of the biometric trait of the authorized user [14].

The Obuda University (OU) biometrics laboratory possesses different biometric recognition devices that can be used in the workplace. The devices are:

- ievo is a company that designs and manufactures biometric fingerprint products. The OU laboratory has ievo ultimate which is a fingerprint reader that provides reliable user identification. It can be used to grant access to buildings and high security areas. It also works in harsh conditions, for this reason it can be used in outdoor and indoor environment. It has a multi spectral imaging sensor that can obtain fingerprints in different conditions such as water, dust, oil, and latex gloves [15]. Table 1 shows ievo ultimate fingerprint reader device.
- Suprema is a company that manufactures different biometric devices used in the work place for access control and time & attendance fingerprint recognition. Suprema's BioEntry Plus, is an IP based fingerprint access control system. It can be used for indoor operations. Suprema's Face Station device provides safety by offering a contactless authentication. This device can be used in facilities where hygiene needs to be enhanced such as hospitals. It has an infrared camera for face recognition and a time and attendance function for worker's time keeping in the workplace [16]. Table 1 shows BioEntry plus fingerprint reader and Face Station facial recognition device.
- UBKEY innovation Inc, is a company that designs iris recognition systems. OU laboratory has mirror key iris recognition devices. These devices capture the image of the person's iris in order to authenticate the identity of an individual and grant access to different locations [17]. Table 1 shows an image of mirror key device.

Biometric technology is a powerful tool in the workplace; however privacy concerns are rising among the implementation of these systems in companies. The acquisition of a biometric trait such as fingerprints or iris that is unique for an individual, poses safety concerns between the workers. It is considered an invasion of their personal privacy; additionally there is a fear that the biometric information collected can be stolen or misused. In order to address these concerns, biometric recognition devices such as suprema's bioentry plus does not save fingerprints images, it stores a fingerprint template that consists of numeric data that cannot be reconstructed into a fingerprint image. This fact protects worker's rights and privacy against the possibility of stolen personal data and the usage of it for other purposes. Moreover, in many U.S. states the employer is liable to maintain the security of the biometric systems and biometric information collected from their employees. It is vital for a

successful implementation of biometric systems in an organization to inform, train the employees about the acquisition processes, the operation of the biometric devices and maintain a balance between monitoring and security.

Table 1: Biometric Equipment

Company	Equipment Name	Equipment Image	Source
uAttend	Fingerprint time clock BN500		[12]
	Facial recognition time clock MN 1000		[12]
Kronos	Kronos InTouch time clock		[13]
Privaris	Plus ID key fob		[18]
Ievo	ievo Ultimate		[15]
Suprema	BioEntry Plus		[16]
	Face Station: Model FSM		Image taken at OU Biometrics Laboratory
UBKEY	Mirror key Iris Recognition System		Image taken at OU Biometrics Laboratory

CONCLUSIONS

Biometric Science and OSH principles have a common goal which is provide an enhanced safety in different areas especially at the work place. Biometrics offers a variety of uses in several fields and is becoming more relevant in the work environment. Fingerprint and facial recognition devices are the most popular used in order to address organizations' needs. The usage of unique human traits to securely authenticate an individual's identity is a valuable safety solution for companies. Biometric recognition allows to securely grant access to authorized personnel into sensitive areas or information, control time and attendance and track employees and processes at all times. In addition, it brings safety to the work environment and promotes a safe culture among the workforce. However, privacy issues regarding the acquisition of biometric traits for different purposes is a concern, it is important to address these concerns and demonstrate how biometric technology protects personal data collected in the workplace.

Biometric systems are becoming relevant in organizations and offer a variety of options tailored to the final user. The challenge of OSH personnel at an enterprise is to choose the correct biometric option that accommodates to the company's requirements and necessities to guarantee a safe and health place for workers.

References

[1] A. K. Jain, A. A. Ross and K. Nandakumar, Introduction to Biometrics, ISBN : 978-0-387-777326-1, New York: Springer, 2011.

[2] B. O. Alli, Fundamental Principles of Occupational Health and Safety. ISBN: 978-92-2-120454-1, Geneva: International Labour Office, 2008.

[3] International Labor Organization, "Guidelines on occupational safety and health management systems, ISBN: 92-2-111634-4," ILO, Geneva, 2001.

[4] T. Vranjes, "Society for Human Resource Management," 16 March 2015. [Online]. Available: https://www.shrm.org/legalissues/stateandlocalresources/pages/workplace-biometric-technology-.aspx. [Accessed 22 April 2016].

[5] Ontario Ministry of Labor, "Ontario Ministry of Labor," 02 October 2013. [Online]. Available: http://www.labour.gov.on.ca/english/hs/faqs/hazards.php. [Accessed 22 April 2016].

[6] Occupational Safety and Health Administration, "Occupational Safety and Health Administration," [Online]. Available: https://www.osha.gov/dte/grant_materials/fy10/sh-20839-10/circle_chart.pdf. [Accessed 21 April 2016].

[7] U.S. Department of Homeland Security, "Immigration Benefits Background Check Systems," Department of Homeland Security, 2010.

[8] Attendance Enterprise , "Biometrics: Advantages for Employee Attendance Verification," Info Tronics Inc, Farmington Hills.

[9] M. James, "10 Ways Biometrics Technology Can Make your Workplace Safer," 11 September 2009. [Online]. Available: http://ezinearticles.com/?10-Ways-Biometrics-Technology-Can-Make-Your-Workplace-Safer&id=2908729. [Accessed 22 April 2016].

[10] American College of Occupational and Environental Medicine, "Biometric Health Screening for Employers," *Journal of Occupational and Environmental Medicine,* vol. 55, 2013.

[11] E. Ross, "Microsoft," 4 April 2016. [Online]. Available: https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-hello-in-enterprise. [Accessed 2 May 2016].

[12] uAttend, "uAttend employee management systems," [Online]. Available: https://www.uattend.com/. [Accessed 06 May 2016].

[13] Kronos Inc, "Kronos Incorporated," [Online]. Available: http://www.kronos.com/. [Accessed 06 May 2016].

[14] M. Prosner, "Automated Buildings," July 2006. [Online]. Available: http://www.automatedbuildings.com/news/jul06/articles/privaris/060629102101privaris.htm. [Accessed 6 May 2016].

[15] ievo, "ievo reader," [Online]. Available: http://ievoreader.com/. [Accessed 16 May 2016].

[16] Suprema, "Suprema Incorporated," [Online]. Available: https://www.supremainc.com/en/AccessControl-TimeandAttendance/Biometric-Devices/FaceStation. [Accessed 16 May 2016].

[17] UBKEY, "UBKEY Innovation," [Online]. Available: http://ubkey.com/eng/ps_all.html. [Accessed 16 May 2016].

[18] IDE, "IDE Inc," [Online]. Available: http://www.ideinc.com/work/privaris-plusid/. [Accessed 16 May 2016].