ADVANTAGES OF ACCESS CONTROL TECHNOLOGIES

Security101®

Security in numbers.
Service that counts.

v01.0

ADVANTAGES OF ACCESS CONTROL TECHNOLOGIES

A growing trend among multiple industries is the move to a more “frictionless” access control security experience; access control that is easy, fast, and convenient to the user, resulting in an experience that does not slow users down. Thanks to advances in technology and improved costs, a variety of efficient, contactless access control solutions have grown in popularity. Considering all options of these solutions is imperative in order to select and implement the perfect system to suit the needs of the organization.

LPR

License plate recognition (LPR) is a unique method of access that utilizes fixed cameras to capture and analyze license plate information in real time to grant entry. Using LPR as a means of granting entry to parking lots and garages for commercial and industrial facilities is useful for employees since they are not required to carry an access card, memorize a PIN code, or attach an adhesive decal. Essentially, the car is the credential. As like many integrated access control systems, the LPR database can tap into the employee list to ensure that only those who are currently employed by the organization may enter.

LPR works by utilizing high definition cameras that are linked with intelligent software that employs specific algorithms as a part of a video analytics system.

In particular, LPR requires an optical character recognition (OCR) engine which deconstructs the images of the license plates and translates it into regular text. The resulting text is matched up to a database of approved registration tags in order to determine which cars are to be granted entry. The speed at which this process occurs is as fast as half-a-second.

Biometrics

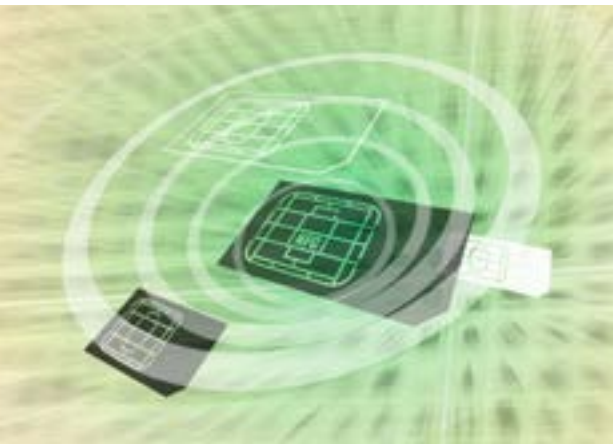
Biometric security has had somewhat of a rocky start over the past decades due to hardware and software shortcomings, like poor processing abilities and inefficient algorithms, resulting in high false acceptance/rejection rates. However in recent years the technology behind biometrics has been refined and improved; for instance, fingerprint recognition in particular has become so efficient that the technology can be found on some of the most popular flagship smartphones.

Today, biometrics are a reality for many organizations that require an additional level of sophisticated security and protection, such as pharmaceutical manufacturing plants. Using biometric credentials as a form of multi-factor authentication of a user is especially popular as an effective form of restricting areas from unauthorized users. For example, in order to be granted access to a secure area, the user must not only present an access card, but they must also press their finger or palm to a biometric reader to complete authentication. There are also biometric readers that can read the veins in one's hand by a simple wave of the hand, no longer requiring the user to physically place their palm in a reader. This process shaves off just a few seconds from each user and ultimately promotes the notion of truly frictionless access control.

Mobile-based access

Now that nearly two-thirds of all working adults own smartphones and typically bring them into the workplace, many organizations are considering utilizing these devices as an access credential. Aside from the cellular antenna, smartphones also contain communication technologies such as Wi-Fi, Bluetooth low energy (BLE), and near field communication (NFC). Wi-Fi can be found in nearly every smartphone and has a very long range of connection; however, locks that rely solely on Wi-Fi are prone to not work if the network is down, and if a malicious user is connected to the network, the phone's credential could be compromised. The advantages of Bluetooth are similar to Wi-Fi; the technology is almost ubiquitous among smartphones sold in the last few years, and with the long read range, the user would be able to keep their smartphones in their pocket or bag and still be able to unlock a door. Most Bluetooth-enabled access control require the user to set up a "gesture" by utilizing a smartphone's gyroscope sensors so that when the user rotates their phone (as if they are turning a doorknob), the door unlocks. NFC works similarly to Bluetooth with two drawbacks: NFC chips are not as prevalent in as many smartphones, and they are limited by a range of a few inches, requiring the user to place their smartphone near the reader in order to gain access, similarly to access cards.

The rising trend of smartphone access control stems from its convenience to the user. Some people's smartphones seem to be permanently attached to their hand; because of this, they are more likely to remember to bring their smartphone with them rather than their access control card when they leave their home or desk.



Likewise, smartphone users are less likely to lend a friend or colleague their phone so they can get access to restricted areas. Furthermore, smartphones can be equipped with a PIN code to gain access to its functions, so in the case of a lost or stolen device, an unauthorized user would not be able to use the phone to gain access to buildings or departments that are restricted. The credentials within the Bluetooth or NFC chip can also be easily deactivated remotely to prevent unauthorized use. Other than convenience, other benefits of these technologies include security personnel/management no longer having to spend time and money on replacement access cards or keys.

The ideal access control system is unobtrusive, user-friendly, and employs state of the art technology as it seamlessly scans the needed credentials to reliably control access to anywhere throughout a facility. This frictionless security experience will likely dominate the manufacturing and industrial sectors over the next few years as managers look to boost employee productivity and overall operational efficiency while also maintaining facility security.